DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA POR MEDIO DE PENTESTING A LAS IP's PÚBLICAS DE LA EMPRESA "ASESORÍAS EN COBRANZAS MEGACOBRO"

ALEXANDER DÍAZ PULIDO
YULIET MARCELA RAMÍREZ RUIZ

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
POSGRADOS
BOGOTÁ D.C.
2017

DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA POR MEDIO DE PENTESTING A LAS IP's PÚBLICAS DE LA EMPRESA "ASESORÍAS EN COBRANZAS MEGACOBRO"

ALEXANDER DÍAZ PULIDO
YULIET MARCELA RAMÍREZ RUIZ

Trabajo de Grado realizado para optar por título de especialistas en Seguridad Informática

Asesor
Álvaro Escobar
Director Especialización Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
POSGRADOS
BOGOTÁ D.C.
2017

Nota de Aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 12 de Agosto de 2017

AGRADECIMIENTOS

Los autores expresan sus más sinceros agradecimientos a:

Dios por permitirnos llegar hasta este momento tan importante y lograr otra meta más en nuestra carrera.

Al Profesor Álvaro Escobar y demás profesores de la especialización, quienes con su apoyo y guía hicieron posible la realización de este proyecto.

A nuestros padres por todo el apoyo brindado que es la base de nuestro empeño para la terminación de este proyecto y estudio profesional.

A La Universidad Piloto de Colombia por ser forjadora de conocimiento en nosotros, una herramienta de saber, para nuestro desarrollo profesional y personal.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

CONFIDENCIALIDAD (ISO 27001): propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[1].

CONTROLES (ISO 27001): las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo[1].

DISPONIBILIDAD (ISO 27001): propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[1].

FIREWALL: es un dispositivo de seguridad de red que controla el tráfico de red, entrante y saliente y decide si bloquear o permitir el tráfico específico basado en un conjunto de reglas configuradas para tal fin[2].

HARDERING: es el proceso de asegurar y reforzar los controles y Seguridad de los Sistemas para mitigar las vulnerabilidades o brechas de Seguridad de la que pueden aprovecharse los atacantes[3].

INTEGRIDAD (ISO 27001): propiedad de la información relativa a su exactitud y complejidad[1].

IP "*INTERNET PROTOCOL"*: es el número de identificación de un dispositivo en una red[4].

IP PÚBLICA: es el número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red, este número identifica el punto de enlace con Internet[5].

LAN "*Local Area Network":* red que conecta ordenadores en una red local[6].

---

[1] ISO 27000.ES, GLOSARIO, Disponible en Internet: http://www.iso27000.es/glosario.html#section10c.

[2] CISCO. ¿Qué es un Firewall? Actualizado, Disponible en Internet: http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

[3] BLOG SMARTEKH. Tips tecnológicos, de configuración y negocio que complementan tu seguridad. 3 de mayo de 2012, Disponible en Internet: http://blog.smartekh.com/que-es-hardening.

[4] BLOG.VERMIIP.ES. ¿Qué es el número IP? ¿Qué significa IP? ¿Qué es una dirección IP? Disponible en Internet: http://blog.vermiip.es/2008/03/11/que-es-el-numero-ip-que-significa-ip/

[5] Herramienta on-line. Disponible en Internet: http://cual-es-mi-ip-publica.com/.

[6] MASADELANTE.COM. ¿Qué es una red LAN? Disponible en internet: http://www.masadelante.com/faqs/lan.

PENTESTING: testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas[7].

RIESGOS (ISO 27001): posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[1].

RIESGO RESIDUAL (ISO 27001): el riesgo que permanece tras el tratamiento del riesgo[1].

SEGURIDAD DE LA INFORMACIÓN (ISO 27001): preservación de la confidencialidad, integridad y disponibilidad de la información[1].

SOFTWARE: es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora[8].

VULNERABILIDAD (ISO 27001): debilidad de un activo o control que puede ser explotada por una o más amenazas[1].

[7] A. ESAU. ¿Qué es Pentesting? Argentina, 12 de junio de 2015. Disponible en Internet: https://openwebinars.net/blog/que-es-el-pentesting/

[8] PEREZ PORTO, Julián. 2008. Definición.de. Disponible en Internet: http://definicion.de/software/

INTRODUCCIÓN

ASESORÍAS EN COBRANZAS MEGACOBRO, es una empresa líder en la recuperación de cartera y servicios de call center, cuenta actualmente con una amplia experiencia y operación, gracias a la estructuración adecuada en la que manejan todos sus servicios, comprometidos con calidad, rendimiento y resultados óptimos para todos sus clientes.

En la ciudad de Bogotá, esta empresa cuenta con el 65% de su operación comercial, lo que le permite manejar un alto volumen de información de sus clientes, información que debe llevar por MEGACOBRO, un tratamiento especial y confidencial en todos los sentidos y áreas, siendo así, el departamento de sistemas tiene un gran reto, proteger esta confidencialidad y dar una adecuada manipulación de los datos, actividad vital para conservar la buena reputación de la compañía y cumplir con las expectativas de quienes han puesto su confianza en ella, sus mejores aliados: los clientes.

En el documento presentado, se resalta esa gran necesidad y se adhiere a ese objetivo de la organización, planteando la evaluación externa de la seguridad en sus IP's públicas, en busca de posibles vulnerabilidades que a su vez conlleven a analizar, de la mejor manera posible, los controles con los que la compañía podría mitigar sus riesgos externos y obtener un nivel mayor de complacencia en la prestación de sus diferentes servicios.

1. JUSTIFICACIÓN

El proyecto tiene como fin, ofrecer un diagnóstico de la seguridad informática desde internet hacia el interior de la LAN de la compañía, verificando la protección que tiene sus configuraciones perimetrales, identificando las posibles vulnerabilidades de sus accesos desde las IP´s públicas y finalmente, proponer sugerencias de mitigación de vulnerabilidades para mejorar la protección de la información interna.

Teniendo en cuenta, como definición de seguridad informática, el conjunto de medidas para la prevención, detección y corrección de incidentes, orientadas a proteger la C*onfidencialidad, Integridad y Disponibilidad* de los activos de la información, lo que significa, en resumen, evaluar el estado actual de sus accesos a aplicaciones por IP's pública y sus vulnerabilidades frente a las posibles medidas de mitigación que se propongan como resultado del análisis de intrusión.

Dentro del proyecto se plantea, no solo realizar la prueba de intrusión controlada a la infraestructura tecnológica (accesos IP´s públicas) y la identificación de vulnerabilidades existentes, sino que también se pretende conforme a los hallazgos, realizar un informe que sugiera una mejora en el sistema de seguridad informática, capaz de mitigar la vulnerabilidad y el riesgo residual, disminuyendo en lo posible el impacto al negocio frente a potenciales ataques externos.

Idealmente, los objetivos del proyecto buscan ayudar a la empresa en la conservación de la tranquilidad dada a sus clientes con el tratamiento de la información y la confidencialidad brindada a la misma, abarcando en gran manera la necesidad de conservar la confianza en el sector y actividad comercial que realiza.

2. PLANTEAMIENTO DEL PROBLEMA

Una gran preocupación para las organizaciones y que ha aumentado durante estos últimos años, se basa en saber qué tan protegida se encuentra su información frente a posibles ataques externos desde internet, por tal motivo, invierten tiempo, recursos y dinero en identificar las vulnerabilidades de los servicios que ofrecen mediante conexiones hacia internet y posteriormente realizar acciones de remediación, que permitan mitigar el riesgo a un nivel aceptable[9].

Dentro de este escenario, en la compañía ASESORÍAS EN COBRANZAS MEGACOBRO, se han presentado tres (3) eventos de ataques informáticos desde internet, comprobados durante el año 2016; de esta situación, surge la necesidad de identificar las vulnerabilidades de los accesos públicos en los servicios de la compañía y minimizar la brecha existente entre, la seguridad actual provista y la seguridad que se pudiera brindar luego del resultado de pruebas de intrusión.

Frente a la problemática identificada, se propone realizar un Pen Test a las IP´s públicas pertenecientes a la Empresa ASESORÍAS EN COBRANZAS MEGACOBRO, con el fin, de identificar en un panorama más claro las vulnerabilidades de estos accesos externos y de manera controlada simular ataques a las IP´s públicas los cuales pueden suceder en la vida real y ayudar a preparar a la compañía para estos ataques, con los hallazgos obtenidos, realizar un análisis y finalmente presentar un informe para la compañía con las posibles remediaciones que se deben implementar para mitigar los riesgos detectados, fortaleciendo así, el estado de la seguridad de la compañía frente a los ataques provenientes de internet.

2.1 FORMULACIÓN

¿Son las IP's públicas de la empresa ASESORÍAS EN COBRANZAS MEGACOBRO, vulnerables a posibles ataques de intrusión que puedan comprometerla internamente?

[9] BOLÍVAR, Carlos. EL TIEMPO, “Cinco Consejos para estar preparado ante amenazas de la red”. Bogotá D.C., 13 mayo de 2014. Disponible en internet: http://www.eltiempo.com/archivo/documento/CMS-13981015

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diagnosticar la Seguridad Informática por medio de un Pentesting a las IP's públicas de la empresa, en busca de posibles vulnerabilidades con el fin de sugerir remediaciones basado en los resultados obtenidos.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un cronograma de Pentesting para la ejecución de ataques controlados a las IP´s públicas de la compañía.

- Seleccionar una metodología para el test de intrusión.

- Ejecutar un plan de pruebas de intrusión de acuerdo con la metodología seleccionada.

- Analizar los hallazgos encontrados con el test de intrusión.

- Presentar un informe de sugerencias de remediación y/o conclusiones frente a los datos arrojados en la evaluación.

4. MARCO REFERENCIA

4.1 HISTORIA

ASESORÍAS EN COBRANZAS MEGACOBRO, es una empresa de cobranzas que cuenta con 30 años de experiencia en esta actividad, es una empresa líder en la recuperación de cartera y servicios de call center, que soporta su operación en una alta experiencia y una fuerte estructura de servicio. Fue fundada en 1986. Actualmente, hace parte del Grupo Bolívar que se caracteriza por reunir empresas y hacer inversiones en diferentes sectores de la economía, tiene presencia en las principales ciudades del país.

4.2 ESTADO ACTUAL

Actualmente ASESORÍAS EN COBRANZAS MEGACOBRO, cuenta con una infraestructura muy robusta la cual provee los servicios necesarios para su operación en Bogotá y 17 regionales del país, dentro de esta infraestructura, la preocupación constante surge en los accesos a los servicios publicados en internet, los cuales son propensos a ataques informáticos y pueden permitir acceso por medios de sus IP públicas.

Existe una estadística parcial de los ataques realizados a la infraestructura de la empresa, los cuales hasta ahora no han sido de impacto considerable, pero si han generado una alerta para el mejoramiento y la aplicación de acciones de mitigación de este riesgo.

Se identificaron 10 ataques durante el 2016, 3 de ellos fueron exitosos y comprometieron la Confidencialidad, Integridad y Disponibilidad de la información; el primero genero un daño en la configuración de troncales SIP de un servidor telefónico, provocando falla en el servicio y la necesidad de formateo completo del servidor para así restaurar el servicio, garantizando el cierre de puertas abiertas en las configuraciones del servidor comprometido; el segundo generó una denegación de servicio, se identificó un procedimiento de acceso por fuerza bruta a uno de los aplicativos del sistema, se procedió así, a la restauración y generación de vaneo de IP´s detectadas en los logs del servidor y del firewall de la compañía; por último, se presentó un secuestro de información ocasionado por un virus “*Ransomware*”, el cual comprometió los archivos de funcionarios directivos, provocado por la descarga del virus a través de correos dudosos que fueron abiertos. Estos ejemplos, son tan solo una muestra de ataques exitosos identificados, los otros 7 eventos generaron una alerta, pero fueron contenidos a tiempo, lo que ayudo a evitar que la infraestructura y los datos se vieran afectados.

Por lo tanto, los antecedentes son un indicador importante en la organización, la cual observa con preocupación un riesgo a sus operaciones ocasionado por los ataques externos y una oportunidad de mejora con la realización de un análisis profundo de las posibles vulnerabilidades y remediaciones que un pentesting pueda proveer.

5. MARCO TEÓRICO

Si bien hasta ahora se ha definido el problema que se desea abordar, se requiere también la ejecución de una metodología aplicada, la cual está basada en distintas definiciones requeridas para el entendimiento del tema.

5.1 EVALUACIÓN DE SEGURIDAD

En el ámbito corporativo, la razón de evaluación de la seguridad es muy común y la necesidad de realizarla, en ocasiones, está ligado a cuestiones de cumplimiento de regulaciones y leyes que lo cobijan, por ejemplo: si la compañía opera con datos personales debe cumplir con las leyes de "*protección de datos personales ley* 1581". Esto implica, que se debe orientar todos los recursos en realizar una debida protección y asegurar los datos personales que serán los activos de la organización, por otro lado, la evaluación de la seguridad está tomando cada vez mayor fuerza en la actualidad, debido a la conciencia que se está generando en el mundo por los riesgos de los activos de información y de los impactos generados tras una mala protección y evaluación de riesgos asociados.

Los autores HÉCTOR JARA y FEDERICO G. PACHECO, dos grandes expertos, consultores, docentes de prestigiosas Universidades en Argentina y especialistas en Seguridad de la información[10], también escritores del libro: "ETHICAL HACKING 2" en dónde describen la evaluación de la seguridad, como: *"una imagen instantánea, una fotografía de la postura de seguridad de la organización en un momento determinado"*[11], por lo que la evaluación por sí sola no genera un valor si no se construye una solución de funcionalidad en el tiempo, que garantice que las recomendaciones sean implementadas y sostenibles.

Dentro del proceso que se ha definido en "diagnosticar la seguridad", se encuentran también varios métodos, en estos se debe buscar el más apropiado para obtener el objetivo a medir, entre ellos se definen las Evaluaciones de vulnerabilidades (vulnerability assessment), Análisis de brecha de cumplimiento y los test de intrusión (pentesting).

5.1.1 Evaluaciones de vulnerabilidades (vulnerability assessment).

Se refiere a la búsqueda de debilidades de los sistemas, más específicamente a su identificación, teniendo en cuenta, su potencial de riesgo más no su confirmación existencial en

[10] Perfiles consultados y disponibles en los links de Internet: Federico G. Pacheco - http://linkd.in/Onqtn0 y Héctor Jara - http://linkd.in/qwjAVD.

[11] JARA, Héctor y PACHECO, Federico G: "ETHICAL HACKING 2: Implementación de un sistema de gestión de la seguridad". 2da Edición, octubre 2013.

el sistema a evaluar, es decir, cuando se identificada una vulnerabilidad esta se reporta, pero no se explora para validar si existe un impacto real.

5.1.2 Análisis de brecha de cumplimiento. Este análisis define la diferencia y la distancia entre el estado actual de la seguridad de la información y el estado deseable que la compañía quiere alcanzar, por lo general, regido por los estándares o regulaciones que la empresa desea cumplir.

5.1.3 Test de intrusión (pentesting). A diferencia de la evaluación de vulnerabilidad, el test de penetración o Intrusión realiza la explotación de las vulnerabilidades encontradas para conocer el impacto real en la organización, esto brinda la posibilidad de generar mecanismos de defensa a profundidad dado que una vulnerabilidad no siempre impacta o es crítica para el negocio de la misma manera de acuerdo con los controles relacionados y a la particularidad de la organización.

5.1.3.1 Tipos de Test de Intrusión. Dentro de los alcances definidos el test de intrusión puede realizarse de distintas maneras, existen el tipo White box o definidos, el cual cuenta con la información de insumo para realizar las labores de intrusión, es decir, se cuenta con la información de infraestructura, aplicaciones y datos que permiten facilitar la labor, en segunda instancia, se presenta el tipo black box o blind, que al contrario del inicial no se cuenta con ningún tipo de información para la exploración, lo que significa que se realizara una labor de intrusión más real a los sistemas, y finalmente, en el tercer tipo se encuentra el grey box, el cual cuenta con una cierta información la cual le permite explorar un tipo de vulnerabilidades, como ejemplo: intentar subir privilegios de usuarios con el conocimiento de uno de ellos.

5.1.3.2 Tipos de enfoque. Los tipos de enfoque son los siguientes: Caja Negra, Caja Blanca y Caja Gris.

- Caja Negra (*black-box*): El ejecutor del test de intrusión no tiene conocimiento sobre el sistema de información a revisar. En general, suele ser el escenario de trabajo cuando la organización responsable del sistema de información contrata a un tercero y la realización del test de intrusión se hace desde el punto de vista de un atacante externo.

- Caja Blanca (White-box): El ejecutor del test de intrusión dispone de un conocimiento detallado del funcionamiento y características del sistema, arquitectura de red, sistemas operativos y software utilizado, etc.

- Caja Gris (Gray-box): Escenario cuando el ejecutor del test de intrusión simula la posición de un empleado interno de la organización que dispone de cierta información (por ejemplo, un usuario y contraseña de un sistema), pero "sin privilegios". El objetivo de este tipo de test de intrusión es detectar vulnerabilidades que permitan elevaciones de privilegios de dichos usuarios.

5.2 ALCANCE Y OBJETIVOS

Es importante tener definido el alcance deseado de un test de intrusión antes de llevarlo a cabo ya que este puede ser amplio, llegando incluso a cubrir toda la infraestructura tecnológica completa de la organización, o, por el contrario, puede estar focalizado en un determinado sistema, equipo y/o aplicación sobre el cual se requiera llevar un control más exhaustivo.
Adicionalmente, una vez definido el alcance, se deben dar respuesta a cuestiones como:

Horario de realización del Test de Intrusión (durante las horas laborales o fuera del horario laboral).

¿Está permitido llevar a cabo denegaciones de servicio (DoS)?
¿Está permitido instalar backdoors?
¿Está permitido realizar defacement de las aplicaciones web?
¿Está permitido llevar a cabo borrados de posibles logs?
¿El personal de la organización tendrá conocimiento de la realización del test de intrusión?
¿Es posible llevar a cabo técnicas de ingeniería social?

5.3 ACTIVIDAD HACKER POR PAÍSES

Según los datos encontrados en la página web "*www.gitsinformatica.com*[12]", de acuerdo con la actividad del hacker y según estudios realizados en informes de empresas de este ámbito, existen pocas estadísticas claras que pueden existir sobre la actividad hacker, uno de los primeros informes en señalar a Colombia como productor de ataques informáticos es Verizon.

Según expertos en seguridad informática de la empresa Xifra, los ataques de "hackers" a equipos informáticos se incrementarán durante los próximos años por el aumento de visitas en páginas web que ofrecen herramientas y técnicas de asalto avanzado.

Este hecho que permite que cualquier interesado pueda acceder a conocimientos antes reservados sólo a expertos. Las acciones más habituales de los "hackers"

[12] Fuente www.gitsinformatica.com

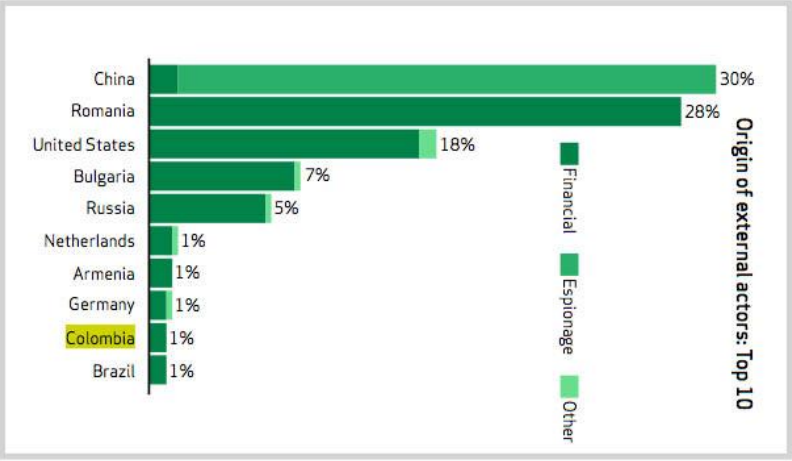
son la sustracción de datos, el robo económico o la creación de virus, troyanos o gusanos.
El informe de Verizon, sin embargo, explica que son al menos 41 las naciones que producen ataques. Colombia ocupa el noveno lugar. China, con el 38 por ciento ocupa el primer puesto seguido de Rumania y Estados Unidos. Ver Ilustración 1. Top 10 de países con más generación de ciberataques.

Colombia es el primer país latinoamericano señalado de atacar empresas. Incluso por encima de Brasil (10) y países como Argentina y Venezuela.

El informe Verizon recopiló 621 casos de pérdida de información de compañías y más de 47.000 reportes de incidentes de seguridad que incluyen ataques de denegación de servicio, robo de datos, espionaje, entre otros.

China es uno de los países del mundo donde más ataques cibercriminales se realizan, según recoge Bloomberg. Los delincuentes cibernéticos pueden lanzar ataques on line desde ordenadores infectados en todo el mundo, por lo que conocer el país de origen puede proporcionar una importante pista en última instancia, determinar la identidad de un hacker.

Ilustración 1. Top 10 de países con más generación de ciberataques



Fuente: Disponible en internet: http://www.gitsinformatica.com/hackers.html.

Bloomberg también evidencia, que Hungría representó el 1,4 por ciento de los ciberataques, con datos del cuarto trimestre de 2012, poniendo al país en la décima posición. Supera a Corea del Sur, aunque por poco. Por su parte, India representó el 2,3 por ciento de los ciberataques del mundo durante el cuarto trimestre de 2012, poniendo al país en el octavo lugar.

Rusia representó el 4,3 por ciento de los ciberataques mundiales durante el cuarto trimestre de 2012, situando al país en el cuarto lugar. Al menos 40 empresas, entre las que se incluyen a Apple, Facebook y Twitter, fueron blanco de los ataques de malware vinculados a un grupo criminal cibernético con sede en Rusia o Europa del Este.

Si China encabeza la lista, Estados Unidos estaría en segundo lugar. Los EE.UU. representaron el 10 por ciento de los ataques al tráfico en el mundo durante el cuarto trimestre de 2012.

Teniendo en cuenta, la información estadística brindada en el estudio anterior, se evidencia que las empresas están potencialmente expuestas, el aumento en sí del ciber-delito, ya abre una brecha en la seguridad de la información, confrontarla y minimizarla a un nivel aceptable, es el reto al que se enfrentan las áreas de sistemas de las compañías, las cuales tendrán también por tarea el incremento de la protección a la misma medida que evoluciona la tecnología y los desarrollos de software de los atacantes.

6. METODOLOGÍAS

Dentro de las metodologías de referencia estudiadas para el propósito del Pentesting están:

6.1 OSSTMM (Open Source Security Testing Methodology Manual)

Manual de la metodología abierta de testeo de seguridad de ISECOM[13]. Es un estándar profesional para el testeo de seguridad en cualquier entorno, desde el exterior al interior, incluye los lineamientos de acción, la ética del testeador, la legislación sobre testeo de seguridad y un conjunto integral de test; El OSSTMM intenta ser un manual de referencia profesional.

Dentro de los objetivos de esta metodología se pueden encontrar:

- Ser un documento de referencia de extremo a extremo para realizar evaluación de la seguridad.
- Estandarizar el proceso de evaluación del Sistema de Seguridad de la información.
- Establecer un nivel mínimo de proceso aceptable.
- Ser una línea base en la que se determine el alcance de la evaluación, es decir, cómo puede o debería ser realizada.
- Fortalecer los procesos y tecnologías de seguridad existentes.
- Evaluar las salvaguardas desplegadas contra el acceso no autorizado.
- Ser una referencia para la implementación de la seguridad de la información.

De igual manera, como lo estipula en el libro OSSTMM vs 2.1, esta metodología consiste en módulos que se encuentran distribuidos según la sección que se esté desarrollando, las secciones con sus módulos se mencionan a continuación:

- Sección A -Seguridad de la Información

Revisión de la Inteligencia Competitiva.
Revisión de Privacidad.
Recolección de Documentos.

- Sección B – Seguridad de los Procesos

Testeo de Solicitud.
Testeo de Sugerencia Dirigida.
Testeo de las Personas Confiables.

[13] HERSON, Pete, Institute for Security and Open Methodologies. Agosto 2003. Disponible en Internet: https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/OSSTMM.es.2.1.pdf

- Sección C – Seguridad en las tecnologías de Internet

Logística y Controles.
Exploración de Red.
Identificación de los Servicios del Sistema.
Búsqueda de Información Competitiva.
Revisión de Privacidad.
Obtención de Documentos.
Búsqueda y Verificación de Vulnerabilidades.
Testeo de Aplicaciones de Internet.
Enrutamiento.
Testeo de Sistemas Confiados.
Testeo de Control de Acceso.
Testeo de Sistema de Detección de Intrusos.
Testeo de Medidas de Contingencia.
Descifrado de Contraseñas.
Testeo de Denegación de Servicios.
Evaluación de Políticas de Seguridad.

- Sección D – Seguridad en las Comunicaciones

Testeo de PBX.
Testeo del Correo de Voz.
Revisión del FAX.
Testeo del Modem.

- Sección E – Seguridad Inalámbrica

Verificación de Radiación Electromagnética (EMR).
Verificación de Redes Inalámbricas [802.11].
Verificación de Redes Bluetooth.
Verificación de Dispositivos de Entrada Inalámbricos.
Verificación de Dispositivos de Mano Inalámbricos.
Verificación de Comunicaciones sin Cable.
Verificación de Dispositivos de Vigilancia Inalámbricos.
Verificación de Dispositivos de Transacción Inalámbricos.
Verificación de RFID.
Verificación de Sistemas Infrarrojos.
Revisión de Privacidad.

- Sección F – Seguridad Física

Revisión de Perímetro.
Revisión de monitoreo.
Evaluación de Controles de Acceso.
Revisión de Respuesta de Alarmas.
Revisión de Ubicación.
Revisión de Entorno.

6.2 ISSAF (Information Systems Security Assessment Framework)
Es una estructura que clasifica la evaluación de la seguridad del sistema de información en dominios y detalles específicos de evaluación o criterios de prueba para cada uno de estos dominios. Apunta a proporcionar información de campo sobre la evaluación de la seguridad que refleja los escenarios de la vida real.

Esta metodología como lo menciona el libro: "Information Systems Security Assessment Framework ISSAF Draft 0.2.1A"[14]: contiene cuatro fases que son las encargadas de estandarizar en paquetes de trabajo de manera genérica para todas las organizaciones una secuenciación que entregué resultados específicos ya sea entrega o un estado deseado de las actividades realizadas. Los resultados obtenidos de las fases son seguidos de actividades diseñadas para integrar el producto o para mantener el estado alcanzado, factible y eficaz.

Las cuatro fases de esta metodología son: Planeación, Evaluación, Tratamiento, Acreditación y Mantenimiento.

6.2.1 Planeación. En esta fase se busca, reunir información acerca de un panorama real de la infraestructura tecnológica, con el fin de tener una evaluación de posibles riesgos. La metodología trae consigo una serie de preguntas base que pueden apoyar el levantamiento de información, con la cual se espera tener por parte del profesional conclusiones que sirvan en la siguiente etapa. En la etapa de planeación también se tiene en cuenta el incentivo o el patrocinador, y es dónde se determina desde el principio la financiación del proyecto, tratando de identificar áreas de resultado clave que motiven la promoción y el interés de la iniciativa, factores críticos de éxito para de esta manera integrarlos a un resultado económico dentro del negocio. En esta fase, es importante reconocer los recursos a utilizar durante la implementación, estimar e identificar los recursos de cualquier índole (personas, productos, servicios etc.,) que son necesarios para cumplir con las exigencias de la ejecución del proyecto. Los resultados obtenidos del mapeo de recursos y costos deben ayudar a determinar al profesional a restringir o acotar el alcance. En la planeación, se tiene en cuenta el presupuesto a ejecutarse, costos y financiación que hacen factibles el proyecto. También se debe seleccionar las tareas a nivel global e ir desglosándose hasta llegar a paquetes de pequeñas tareas que hagan un esquema de trabajo organizado. En la planeación se debe determinar un responsable o gerente de proyecto, quien es la persona que deberá tomar las decisiones y ser responsable ante el equipo de asignar las tareas y determinar los entregables, como también de llevar la trazabilidad de todas las partes y resolver el esquema propuesto. Cuenta con una evaluación de riesgos, que se integra previo al proyecto con el fin de actuar como una auditoria y

[14] OPEN INFORMATION SYSTEM SECURITY GROUP. Information Systems Security Assessment Framework Mayo 2006, Disponible en Internet:
https://ht.transparencytoolkit.org/FileServer/FileServer/whitepapers/issaf/issaf0.2.1A.pdf

evaluar el estado de la seguridad de la información, es decir, que esta actividad en la planeación incorpora actividades de remediación y tratamiento del riesgo que pueden llegar a ser parte del alcance.

6.2.2 Evaluación. En esta fase proporciona un enfoque que evalúa los riesgos de la seguridad de la información para una empresa. Las evaluaciones de los riesgos se asocian con los objetivos del negocio con el objetivo de que el alcance se alinee para cumplirlos. En la evaluación se presenta también el costo vs el beneficio de la implementación y el mantenimiento de los controles de seguridad de la información, esto teniendo en cuenta que son costos elevados los que generalmente hacen parte de estos proyectos y comparándolos con el impacto de no hacerlo. La fase de evaluación a su vez se divide en dos categorías:

- Identificación del riesgo inherente.
- Evaluación de los controles.

Se realiza una evaluación de amenaza, en esta evaluación se analizan tres aspectos importantes de la fase:

- Evaluación de impacto.
- Evaluación de probabilidad.
- Evaluación de controles.

El resultado de esta tarea se convierte en lo que se conoce como riesgo residual. También, es importante para esta actividad la realización de la evaluación en cuanto a normativa y legislación se refiere, de igual manera las políticas existentes de que rigen y dan lineamientos de la seguridad de la información.

6.2.3 Tratamiento. Esta etapa da una idea del qué hacer con los riesgos residuales, tomar decisiones al respecto de la investigación y en la implementación de salvaguardas o controles que puedan dar un tratamiento adecuado del riesgo. La fase busca, ejecutar los controles de manera tal que el tratamiento sea cual sea, aceptar, mitigar, transferir o eliminar los riesgos evidenciados, tenga efectividad y tenga en cuenta toda la metodología aplicada y los hallazgos encontrados. Para una documentación adecuada de los hallazgos, y decisiones tomadas de acuerdo a los riesgos con el tratamiento, la metodología facilita una plantilla de plan de tratamiento en donde se realiza un plan de trabajo para seleccionar los controles de acuerdo con el tratamiento seleccionado.

6.2.4 Acreditación. Esta etapa implica evaluar los controles que han de ser implementados en las fases anteriores, con el fin de certificar los resultados y dar un alcance a los mismos. Para este punto es necesario contar con una entidad

certificadora que avale las tareas sincronizándolas con los objetivos del negocio y evaluando sus especificaciones y alcance del proyecto. Esta es la parte externa que puede ser neutra en la solución mirando la empresa como una parte integra, pero conociendo su base de negocio y ajustando su alcance conforme a la medida de sus necesidades. Posterior a esta actividad la entidad acreditadora deberá genera un informe detallando los pro y contras, las áreas débiles y los controles adecuados o sobredimensionados que deberían ser reevaluados, esto con el fin de que la organización apruebe y pueda recibir el aval adecuado para la implementación del proyecto.

6.2.5 Mantenimiento. Las organizaciones certificadas por la ISSAF deberán demostrar su Acreditación, ISSAF en forma continua. Para garantizar esto, OISSG llevará a cabo Evaluaciones / revisiones regulares del cumplimiento. La frecuencia de esta revisión se basa en el tamaño de la organización y el alcance de la acreditación.

6.3 OWASP (Open Web Application Security Project)

Es una guía de pruebas de una completa metodología para la revisión y evaluación del estado de seguridad de aplicaciones web[15].

Los materiales están disponibles bajo una cobertura de licencia abierta y libre, enfocada a la seguridad de software seguro en las organizaciones y que puede ser alimentada por personas de todo el mundo con el fin de reforzarla basada en la experiencia.

Por las especificaciones de la metodología (aplicaciones/software), se determina que no es funcional para el proyecto evaluar únicamente la seguridad a nivel de aplicativos de la Compañía.

[15] OWASP, Disponible en Internet: https://www.owasp.org/images/8/80/Gu%c3%ada_de_pruebas_de_OWASP_ver_3.0.pdf

7. SELECCIÓN DE LA METODOLOGÍA

Realizando la revisión de las metodologías descritas anteriormente, para la ejecución del Pentest, se evidencio que tienen similitudes en la manera de ejecutar las actividades de búsqueda de vulnerabilidades (fases del test), por lo tanto, se tomó lo que para este ejercicio es aplicable y se generaron las siguientes fases:

7.1 FASE DE DESCUBRIMIENTO

Teniendo en cuenta que se quiere simular en mayor medida la forma como un atacante recopila la información necesaria de su objetivo, así mismo en la fase de descubrimiento se desea recopilar y documentar por medio de diferentes medios de internet (páginas de la compañía, noticias, cuentas de correos electrónicos, páginas como whois y central opps), toda clase de información concerniente al objetivo de este ejercicio. Esta fase también llamada Footprinting es el primer paso que se debe ejecutar en el test de intrusión y hace referencia al enfoque de caja negra.

7.2 FASE DE ANÁLISIS Y PLANEACIÓN

En esta fase el enfoque cambia de caja negra a caja gris, en el cual se realiza una comparación de la información recopilada en el footprinting con la información real acerca de las IP´s públicas, en esta fase se realiza un inventario de las IP's y se realiza un cronograma de pruebas controladas.

7.3 FASE DE ESCANEO

Con la información organizada de las IP's públicas de la compañía se procede a realizar varias actividades de escaneo:

- Identificación de Sistemas activos.
- Identificación de Puertos abiertos.
- Identificación de Sistemas Operativos.
- Identificación de Aplicaciones.
- Escaneo de Vulnerabilidades.
- Identificación de vectores de Ataque.

Esta fase también es llamada Fingerprinter, el cual define como es el proceso de determinar información cómo el sistema operativo que se utiliza en un host remoto, puertos servicios, etc. Esto se lleva a cabo mediante el análisis de los paquetes recibidos desde el host en cuestión. Hay dos formas distintas a OS huella digital, de forma activa (es decir, NMAP) o pasivamente (es decir scanrand).

En el último paso de la fase de escaneo, se realiza la identificación de vectores de ataque, donde se pretende generar diferentes hipótesis de los posibles caminos que el atacante o el pentester aplicará para lanzar un ataque en función de las vulnerabilidades detectadas.

7.4 FASE DE EVALUACIÓN

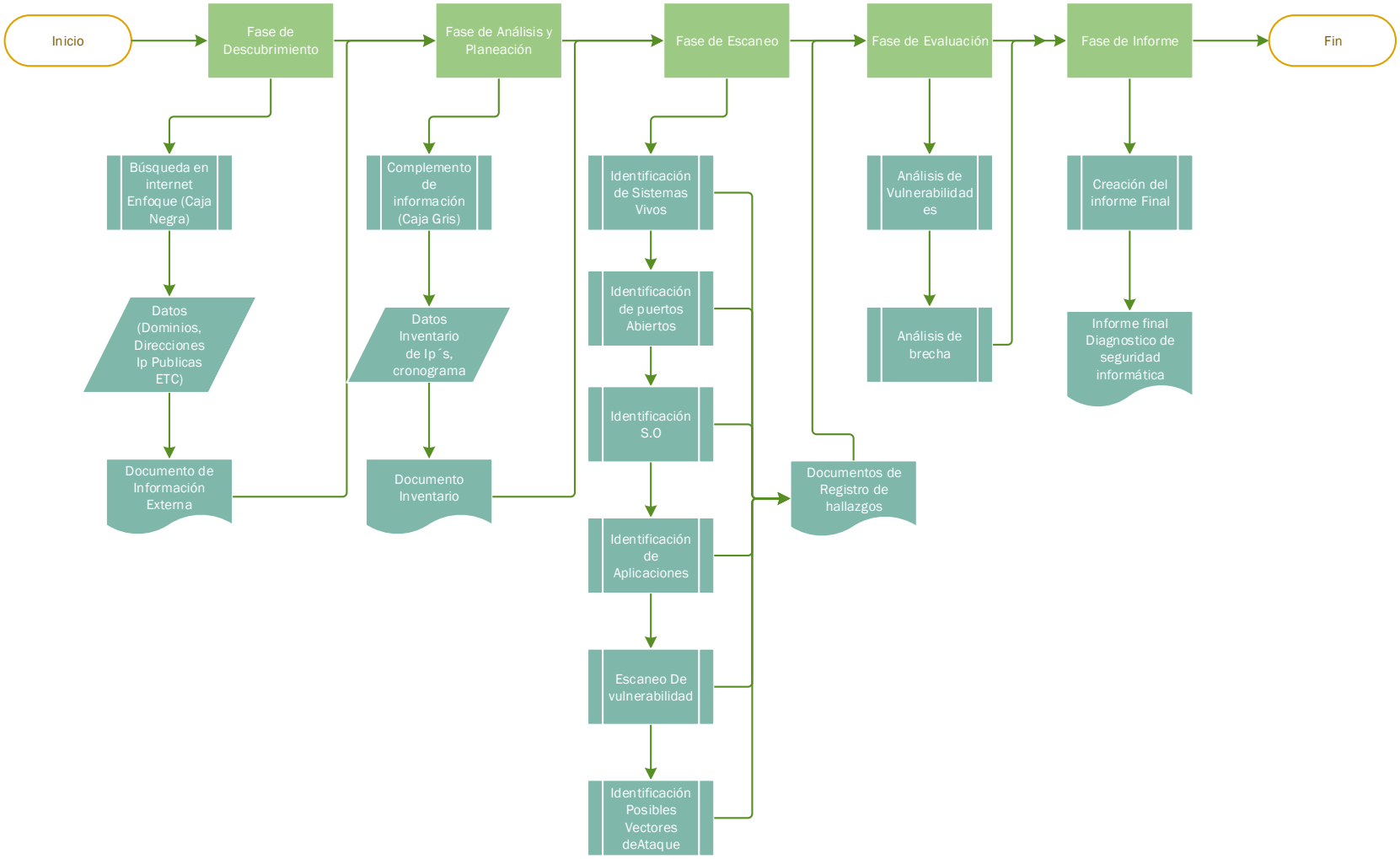
Para esta fase, es muy importante haber identificado y recopilado plenamente toda la información necesaria para analizar y determinar si las vulnerabilidades encontradas podrían ser explotadas por los atacantes y eventualmente obtener acceso a un host de destino en una red y a su información.

7.5 FASE DE INFORME

Como el propósito de este test de intrusión es diagnosticar seguridad informática desde accesos de internet, se presentará a la compañía los hallazgos por medio de un informe con los resultados obtenidos y las recomendaciones consideradas adecuadas para que la brecha de seguridad sea más pequeña y minimizar el posible riesgo de ataques externos. Ver Anexo D Informe Final

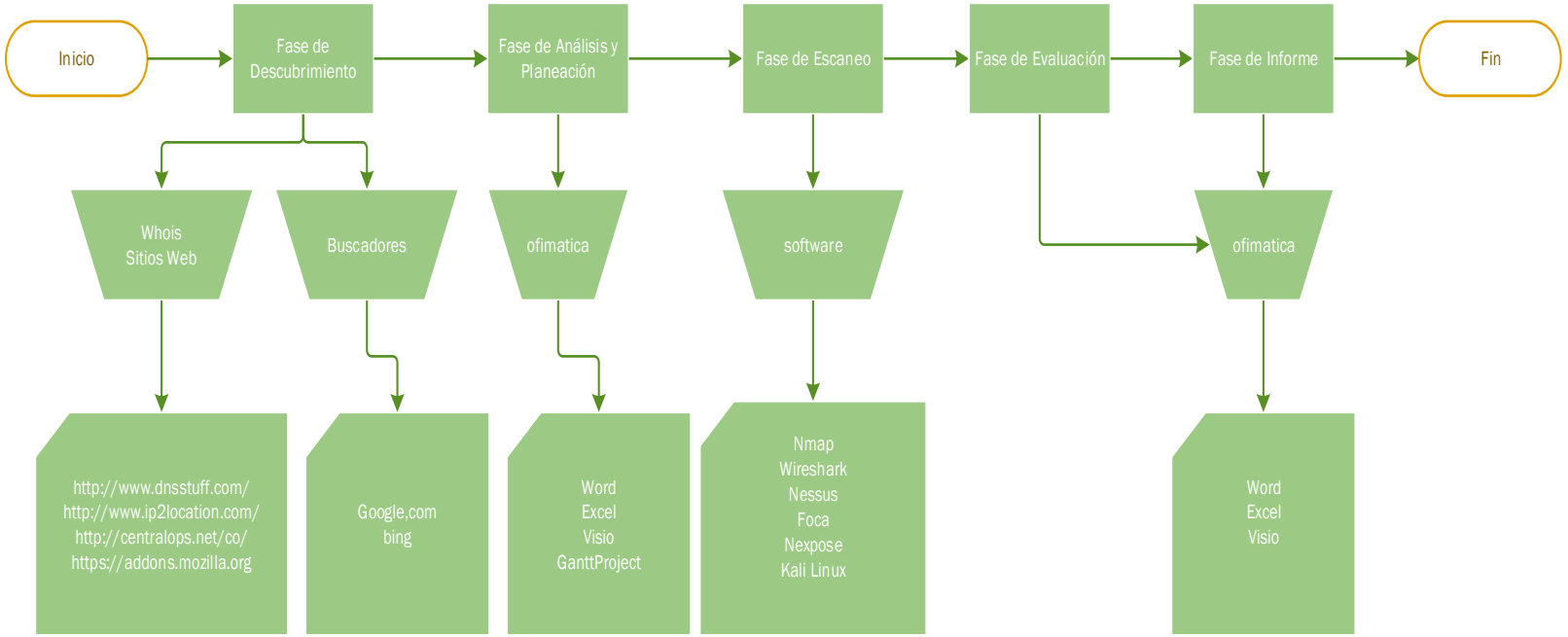
El resumen de la metodología seleccionada se puede observar como la consecución lineal de algunas actividades y de igual manera del uso de las herramientas de software propias de cada actividad. Ver Ilustración 2. Fases del proceso de Pentesting y ver Ilustración 3. Herramientas de uso en el Pentesting

Ilustración 2. Fases del proceso de Pentesting



Fuente: Diseñadores del proyecto.

Ilustración 3. Herramientas de uso en el Pentesting



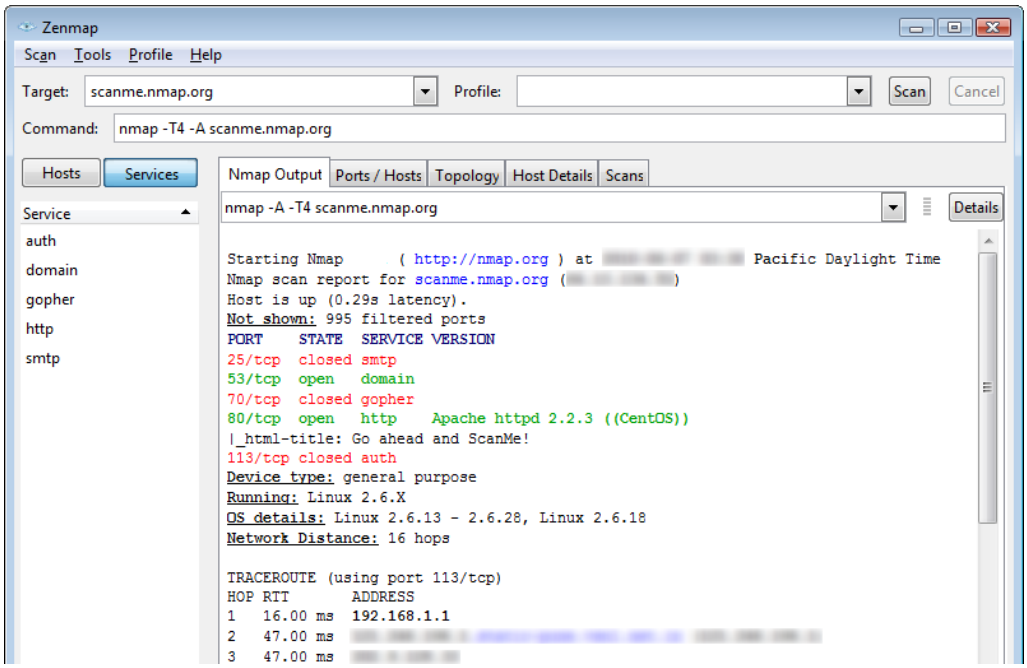
Fuente: Diseñadores del Proyecto.

8. HERRAMIENTAS

8.1 NMAP

Es una herramienta de código abierto para la exploración de red y auditoria de seguridad, se diseñó para analizar rápidamente grandes redes, esta herramienta puede determinar que equipos se encuentran disponibles en una red, que servicios, que sistemas operativos, que tipo de filtros de paquetes o cortafuegos se están utilizando; estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Ver Ilustración 4. Pantallazo herramienta Zenmap Muestra de Interfaz.

Ilustración 4. Pantallazo herramienta Zenmap – Muestra de Interfaz



Fuente: Zenmap, Disponible en https://nmap.org/zenmap/

8.2 FOCA

Es una herramienta de análisis de metadatos para dibujar una red a partir de los metadatos, entre sus funcionalidades permite la búsqueda de documentos con diferentes tipos de ficheros como:

MS Office: doc, docx, xls, xlsx, ppt, pptx, ppsx y pps,
Open Office: odf, ods, odt, odp, sxw, swi y sxc
Adobe: pdf, indd

Otros: wpd, svg y svgz
De igual manera permite, analizar la URL y generar un mapa de los sitios con la siguiente información:

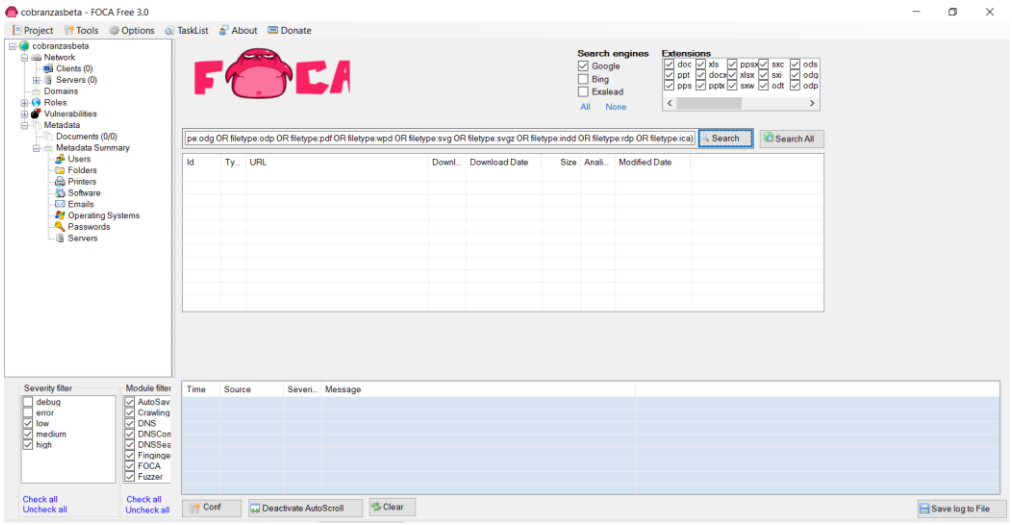
Se extrae el nombre de dominio.
Se busca su dirección IP.

Si está seleccionada la opción de fingerprinting pasivo, se intenta averiguar la tecnología del servidor web y el mapa de directorios como, por ejemplo:

http://www.uno.com/
http://www.uno.com/directorio1/
http://www.uno.com/directorio1/docs/
http://www.uno.com/directorio1/docs/pdf/

Y se darían de alta asociados como directorios al nombre de dominio de www.uno.com. Ver Ilustración 5. Pantallazo herramienta FOCA. Muestra de interfaz

Ilustración 5. Pantallazo herramienta FOCA. Muestra de interfaz



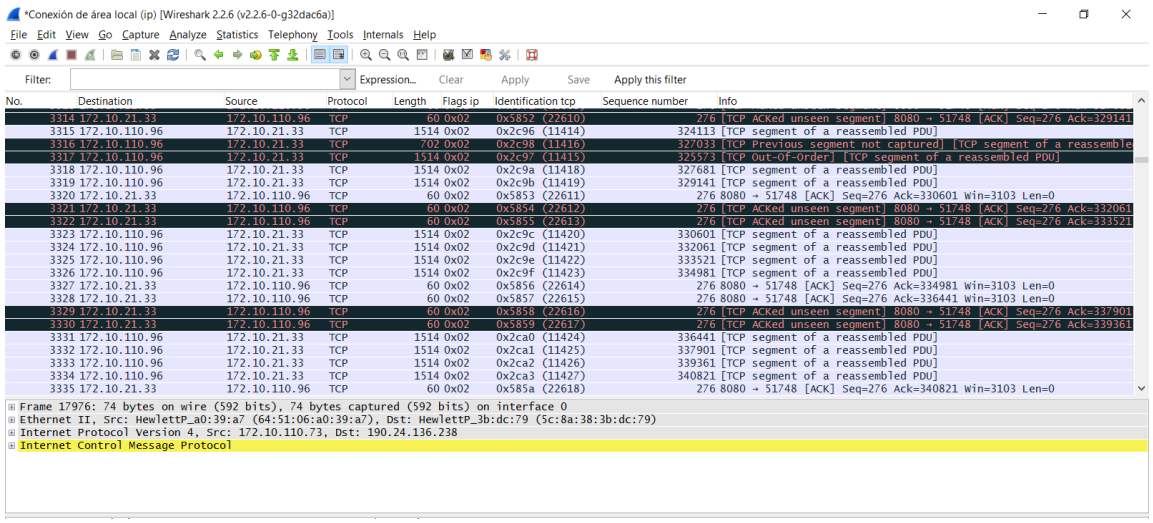
Fuente: FOCA https://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml.

8.3 WIRESHARK

Es un analizador de protocolos de red ampliamente utilizado en el mundo, permite ver lo que está ocurriendo en su red, es utilizado para analizar y detectar problemas en redes de comunicaciones y para analizar los distintos protocolos del

modelo OSI en una conexión real. Ver Ilustración 6. Pantallazo herramienta Wireshark – Muestra de interfaz

Ilustración 6. Pantallazo herramienta Wireshark – Muestra de interfaz



Fuente. Wireshark. https://www.wireshark.org/

8.4 NESSUS

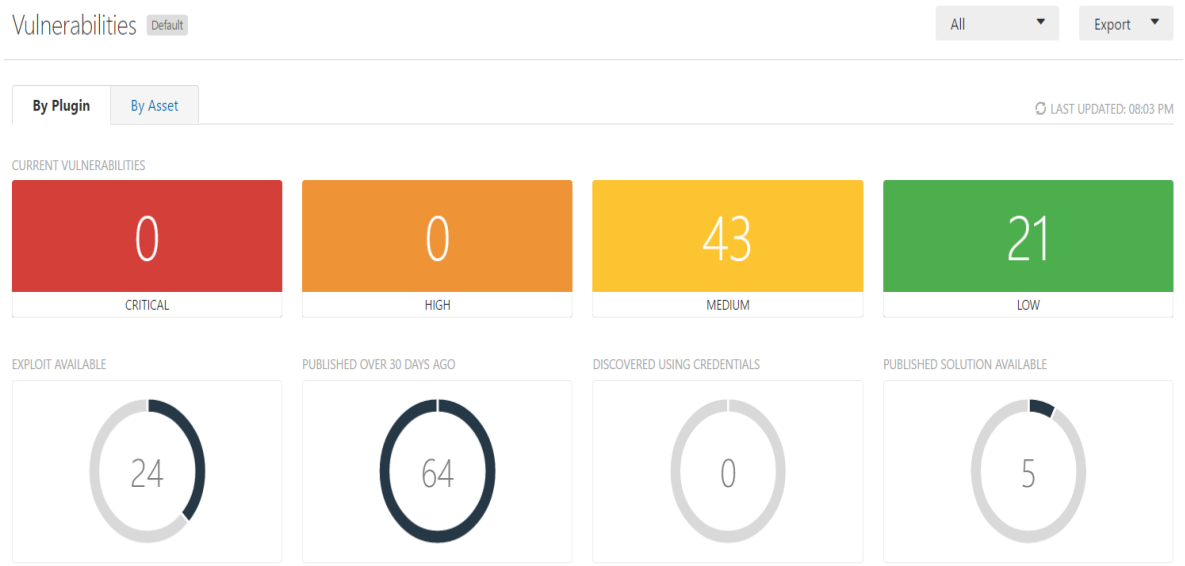
Es una herramienta de escáner de vulnerabilidades más usada, encargada de identificar las debilidades y errores de configuración que los atacantes pueden aprovechar. Ver Ilustración 7. Pantallazo página de ingreso de Nessus

Ilustración 7. Pantallazo página de ingreso de Nessus

Fuente. Disponible en Internet https://cloud.tenable.com/login.html#/.

Una vez se ingresa al dashboard, se evidencian gráficas estadísticas de las vulnerabilidades halladas en el último escaneo realizado a las diferentes IP's. Ver Ilustración 8. Pantallazo de Dashboard de Nessus

Ilustración 8. Pantallazo de Dashboard de Nessus



Fuente. Dashboard Nessus https://www.tenable.com/products/nessus-vulnerability-scanner.

8.5 KALI LINUX

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Este sistema Operativo ofrece excelentes herramientas para la seguridad informática y la auditoría de redes, por lo tanto, hace parte principal del sistema para utilizar en este proyecto. Ver Ilustración 9. Pantallazo de Sistema Operativo Kali Linux

Ilustración 9. Pantallazo de Sistema Operativo Kali Linux

Fuente. Kali Linux. https://www.kali.org/

Al tener en cuenta el uso de estas herramientas, no significa que estas por si solas generen un diagnóstico de la seguridad con los resultados o evidencia de presencia de vulnerabilidades, también es importante un proceso de análisis de los resultados por parte del administrador de seguridad y así sacar provecho de la información encontrada para robustecer los sistemas y limitar la brecha de seguridad a los atacantes y sus posibles vectores de ataque.

9. DESARROLLO DEL PENTEST

9.1 FASE DE DESCUBRIMIENTO

En el desarrollo de esta actividad se hace uso de herramientas como navegadores de internet, redes sociales y otras herramientas públicas para recopilar información de la organización objetivo, es decir, se plantea la necesidad de conocer en mayor medida, ¿quién es la empresa?, sus dominios, sus direcciones IP´s, direcciones de correo, información de funcionarios, etc. Toda la información que pueda estar al alcance del atacante.

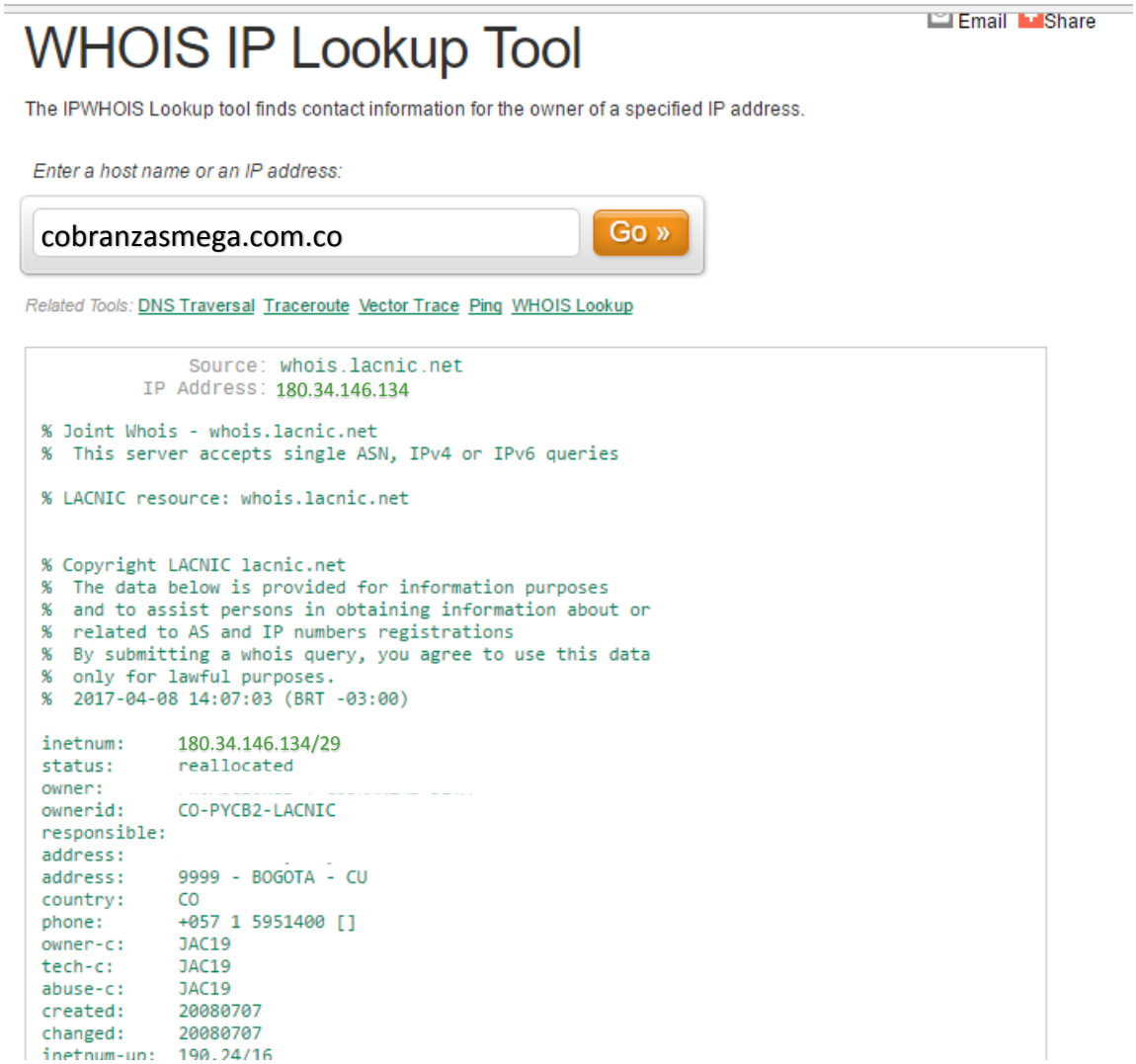
Esta fase es la que mayor tiempo lleva, dado que requiere un alto empeño y tiempos de investigación. Ver Ilustración 10. Pantallazo de la herramienta WHOIS – Consulta de IP/dominio

Ilustración 10. Pantallazo de la herramienta WHOIS – Consulta de IP/dominio

Fuente. Disponible en Internet https://who.is/.

El resultado de la consulta se puede apreciar en la siguiente imagen de la interfaz. Ver Ilustración 11. Pantallazo de resultado de consulta WHOIS

Ilustración 11. Pantallazo de resultado de consulta WHOIS.



Fuente. Disponible en Internet https://who.is/.

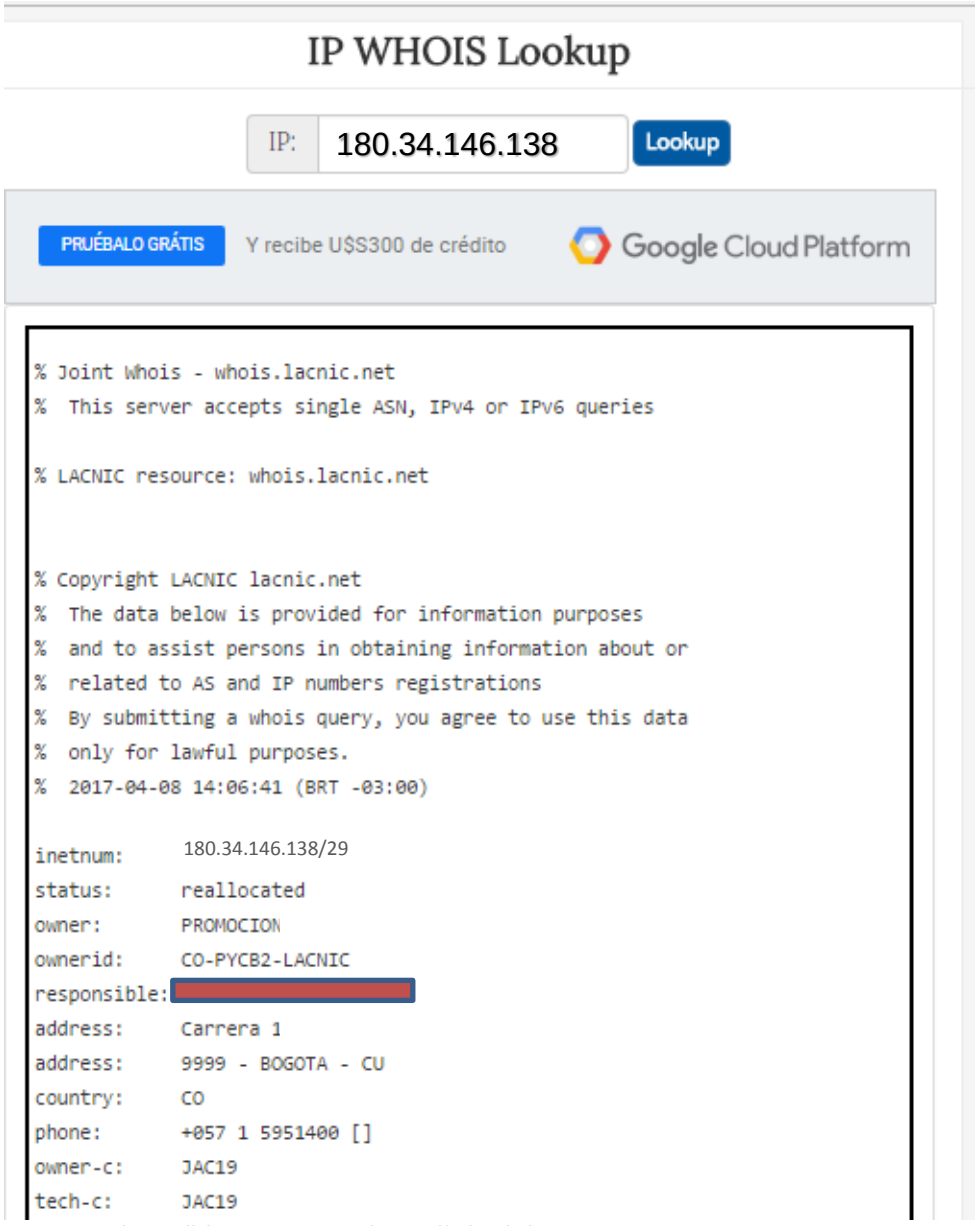
Como se puede evidenciar existe gran cantidad de paginas en internet que permiten la busqueda de informacion con herramientas whois, por lo que un atacante tiene las herramientas para conocer su objetivo y asi analizar la mejor mánera para organizar un ataque a cualquier infraestructura.

En este caso, con la consulta a las paginas que realizan este tipo de búsquedas se pudo encontrar:

- IP pública.
- DNS.
- Direccion de objetivo.

- Direcciones de Correo.
- Nombres de funcionarios.
- Numeros de telefono.
- Registro de dominio y fechas de vigencia del dominio. Ver Ilustración 12. Resultados de la consulta en WHOIS

Ilustración 12. Resultados de la consulta en WHOIS

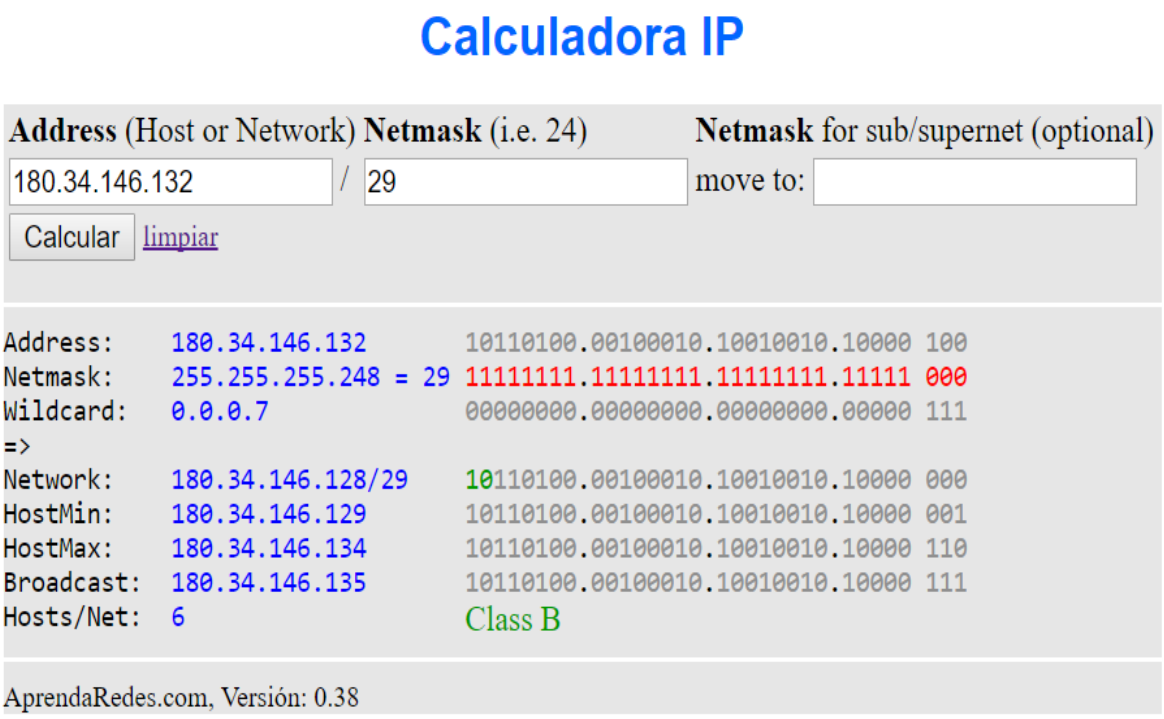


Fuente. Disponible en Internet https://who.is/.

Con este tipo de información Básica y un análisis primario, se puede establecer los rangos de IP´s públicas que son utilizados por la compañía y así tener registro de estos datos para efectos del ejercicio; en la vida real el atacante puede empezar con esta información a realizar un esquema de ataque a su objetivo.

Ejemplo de uso de una calculadora IP para generar el rango de direcciones públicas que pueden tener servicios asociados y ser objetivos de ataque. Ver Ilustración 13. Calculadora IP on-line.

Ilustración 13. Calculadora IP on line

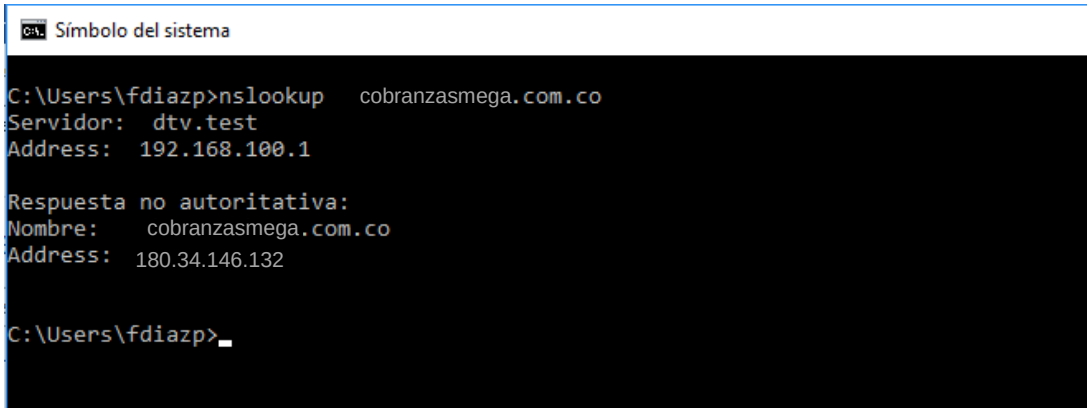


Fuente. Disponible en Internet: http://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi?host=190.24.136.232&mask1=29&mask2=.

La información de la calculadora hace saber el número de host que pueden tener asociados servicios.

De igual manera en cualquier equipo de cómputo se pude hacer uso del comando por consola NSLOOKUP para identificar la dirección IP asociada al dominio. Ver Ilustración 14. Ejemplos de NSLOOKUP.

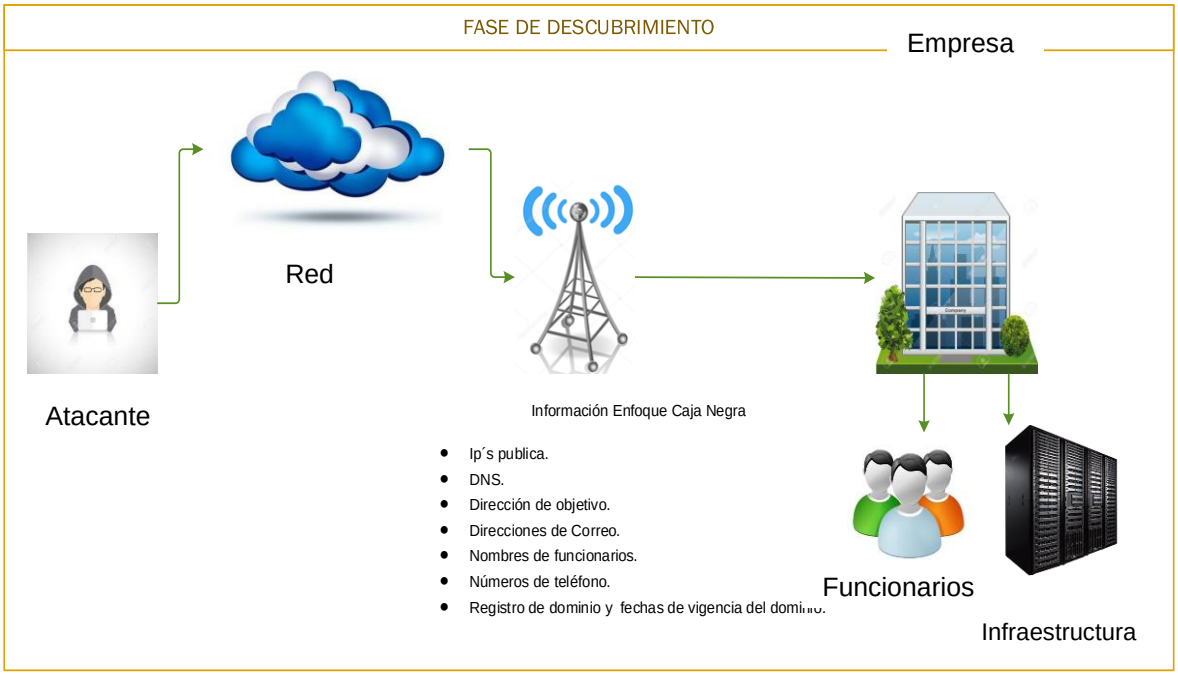
Ilustración 14. Ejemplo de NSLOOKUP



Fuente. Command prompt https://technet.microsoft.com/en-us/library/cc754340(v=ws.11).aspx.

En la etapa de descubrimiento y utilizando el enfoque de caja negra, el atacante puede conocer información básica ingresando a Internet, ahí podrá establecer datos de interés cómo lo son: IP pública de la empresa, dominio, nombre de funcionarios, datos de ubicación, teléfono, estos datos pueden conducir así a información más relevante, el esquema realizado para este escenario es el mostrado en la siguiente ilustración. Ver Ilustración 15. Esquema caja negra.

Ilustración 15. Esquema caja negra



Fuente. Propia de los diseñadores del proyecto.

Tanto como lo puede realizar un atacante, el análisis de enfoque de caja Negra busca la información pública en internet y se obtienen datos preliminares del objetivo.

9.2 FASE DE ANÁLISIS Y PLANEACIÓN

En esta fase se complementa la información y se realiza un inventario de la infraestructura general de las IP´s públicas y los servicios asociados, con los que se realiza la planeación necesaria para llevar a cabo la siguiente fase de escaneo.

El enfoque del Pentest cambia en esta fase de caja negra a caja gris, dado que se complementa la información descubierta en la fase anterior con conocimientos básicos de las IP's públicas, infraestructura, sistemas operativos, servicios y toda información que un atacante pueda utilizar para la realización de ataques.

Para este caso, la misma información puede ser usada para el test de vulnerabilidad y ser un medio de diagnóstico que permita vislumbrar la brecha de seguridad entre el estado actual y el estado futuro e ideal, complicando así al atacante, dado que se ha descubierto las vulnerabilidades y se han aplicado correctivos.

Por lo tanto, la imagen de infraestructura, con el enfoque gris, descubre nuevos elementos y permite visualizar la siguiente etapa del test. Ver Ilustración 16. Esquema caja gris.

Ilustración 16. Esquema caja gris

Fuente. Propia de los diseñadores del proyecto.

Como se muestra en el anterior esquema, ya el atacante no solo tiene a nivel global información básica, sino que también, conoce parte de la infraestructura, sistemas operativos, firewall, etc.

Dentro de la fase se realiza el inventario de las IP´s públicas que se van a evaluar y con esto se planea el levantamiento de la información, en esta actividad se usan plantillas, ver Anexo A, que, en la fase de escaneo, servirán de registro de nueva información encontrada.

Para llevar a cabo el registro se toma como información relevante a registrar:

- Fecha.
- Nombre.
- Fase.
- IP pública y máscara.
- Puertos encontrados.
- Servicios y las URLs.
- Comentarios, diagnósticos, Herramientas.
- Firma de los responsables.

Los formatos registran la información necesaria para llevar un proceso de análisis de manera organizada y permite evidenciar tanto el inventario de IP's a escanear, como las herramientas utilizadas, permitiendo al profesional de seguridad generar un diagnóstico y comentarios que son requeridos en la fase de evaluación.

9.3 FASE DE ESCANEO

Luego de obtener la información requerida en la fase de análisis y planeación, se da inicio a la fase de escaneo, haciendo uso de las planillas creadas y de las herramientas propuestas para poder obtener información que permita evidenciar posibles vulnerabilidades.

Este proceso da inicio, teniendo en cuenta la metodología y la planeación por lo tanto se procede así:

9.3.1 Identificación de Puertos abiertos.

Se realiza el escaneo con la ayuda de la herramienta Nmap sobre cada IP, en donde es posible identificar los puertos abiertos y los servicios que pueden estar asociados.
Con Nmap se hace un escaneo utilizando varios parámetros que proporciona la herramienta como, por ejemplo:

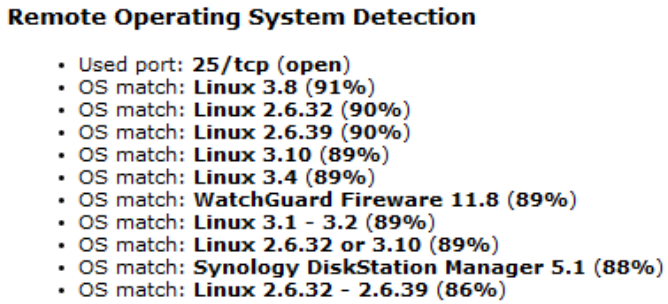
Nmap .T4 -A -v 180.34.146.135
nmap -T4 -A -v -Pn 180.34.146.135
nmap -sS -sU -T4 -A -v 180.34.146.135

nmap -p 1-65535 -T4 -A -v 180.34.146.135

Con estos comandos se puede realizar el levantamiento de información que proporciona la herramienta acerca de los puertos que utiliza.

9.3.2 Identificación de Sistemas Operativos. De la misma manera, como el sistema realiza el análisis de puertos, la herramienta tiene la capacidad de detectar por medio de un porcentaje de compatibilidad que tipo de sistema operativo que está siendo usado en el host escaneado e identificado. Ver Ilustración 17. Reporte de la herramienta Nmap para identificación de S.O.

Ilustración 17. Reporte de la herramienta Nmap para identificación de S.O



Fuente: NMAP https://nmap.org/

9.3.3 Identificación de Aplicaciones. La identificación de aplicaciones se tiene plenamente evidenciada, dado que dentro de la fase de análisis y planeación se cambió el enfoque a caja Gris, lo que implicó realizar un inventario de las IP's y sus servicios asociados.

Sin embargo, teniendo en cuenta que en la vida real un atacante no tiene conocimiento de esta información y su misión es buscar en lo posible las aplicaciones y servicios de su objetivo con el fin de generar vectores de ataque, las herramientas usadas en el pentesting también pueden dar información de los servicios y aplicaciones, por ejemplo, una manera sencilla es la asociación de los puertos escaneados en el proceso anterior, el cual evidencia los posibles servicios; en la Ilustración 16 se evidencian los hallazgos del escaneo, identificando los puertos: 25, 587, 110, 995, 143, los cuales hacen referencia a los protocolos SMTP, POP3 e IMAP, los cuales son servicios de correo.

De igual manera se evidencian los puertos 80 y 443 que hacen referencia a protocolo HTTP y HTTPS, estos, con la simple ejecución de la dirección y el puerto en el navegador web, podría probar el servicio asociado. Ver Ilustración 18. Informe de escaneo de puertos y servicios con una de las IP's Públicas.

Ilustración 18. Informe de escaneo de puertos y servicios con una de las IP's Públicas

Ports

The 991 ports scanned but not shown below are in state: **filtered**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
25	tcp	open	smtp	syn-ack	Postfix smtpd
80	tcp	open	http	syn-ack	
110	tcp	open	pop3	syn-ack	Zimbra pop3d
143	tcp	open	imap	syn-ack	Zimbra imapd
443	tcp	open	http	syn-ack	Zimbra http config
465	tcp	open	smtp	syn-ack	Postfix smtpd
587	tcp	open	smtp	syn-ack	Postfix smtpd
993	tcp	open	imap	syn-ack	Zimbra imapd
995	tcp	open	pop3	syn-ack	Zimbra pop3d

Fuente: Nmap https://nmap.org/.

Dado que la herramienta es tan robusta también asocia los puertos a los servicios conocidos como lo muestra la Ilustración 18.

Estos escaneos con las herramientas Nmap y wireshark generan informes de hallazgos, los cuales, en la fase de evaluación, se toman en cuenta para analizar los datos y concluir en posibles vectores de ataque y las remediaciones necesarias que se aconsejan para fortalecer la seguridad informática de los servicios asociados a las IP's públicas. Ver Anexo B Informe de escaneos con NMAP

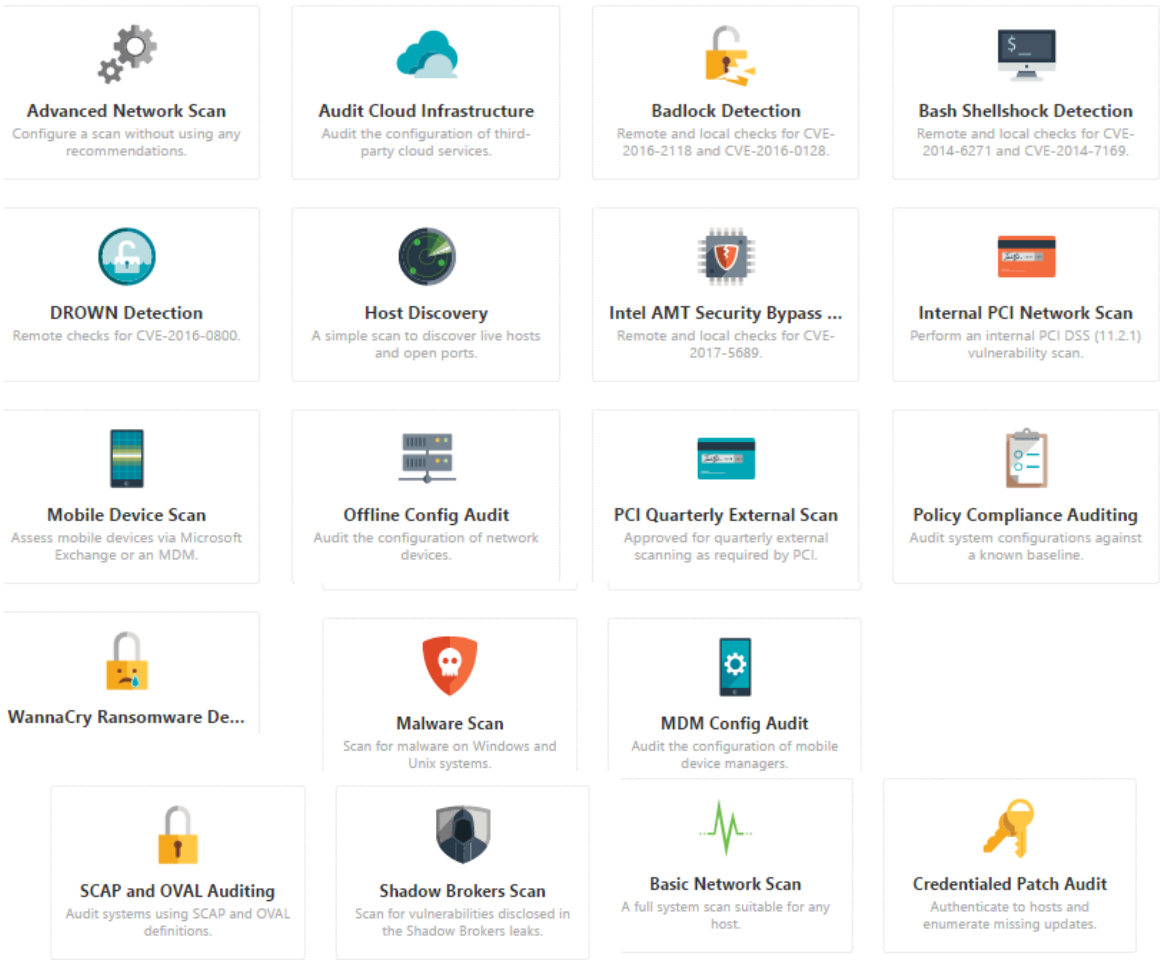
9.3.4 Escaneo de Vulnerabilidades. Esta actividad en la Fase de escaneo es una de las más importantes, debido a que gracias a las herramientas utilizadas y que actualmente se encuentran en el mercado, se puede identificar de manera más rápida las posibles vulnerabilidades que se hallan en los sistemas asociados a las IP's públicas que en este ejercicio de pentesting se están evaluando.

Para el escaneo de vulnerabilidades de esta fase, se realizó un escaneo a cada IP pública para identificar sus vulnerabilidades, teniendo en cuenta las opciones de la herramienta denominadas "Basic Network Scan", "Advanced Network Scan" y "Legancy Web App Scan", que para propósito del pentesting de vulnerabilidad generan información relevante.

También, para reforzar el escaneo y obtener la mayor información posible de la herramienta, se alternaron en diferentes horarios y tipos de escaneos, cambiando los parámetros de búsqueda de los escaneos. Ver ilustración 19. Opciones de escaneo herramienta Nessus, Ver ilustración 20. Escaneos realizados con la plataforma de Nessus online y la ilustración 21 Parametrización de las opciones de escaneo programa Nessus.

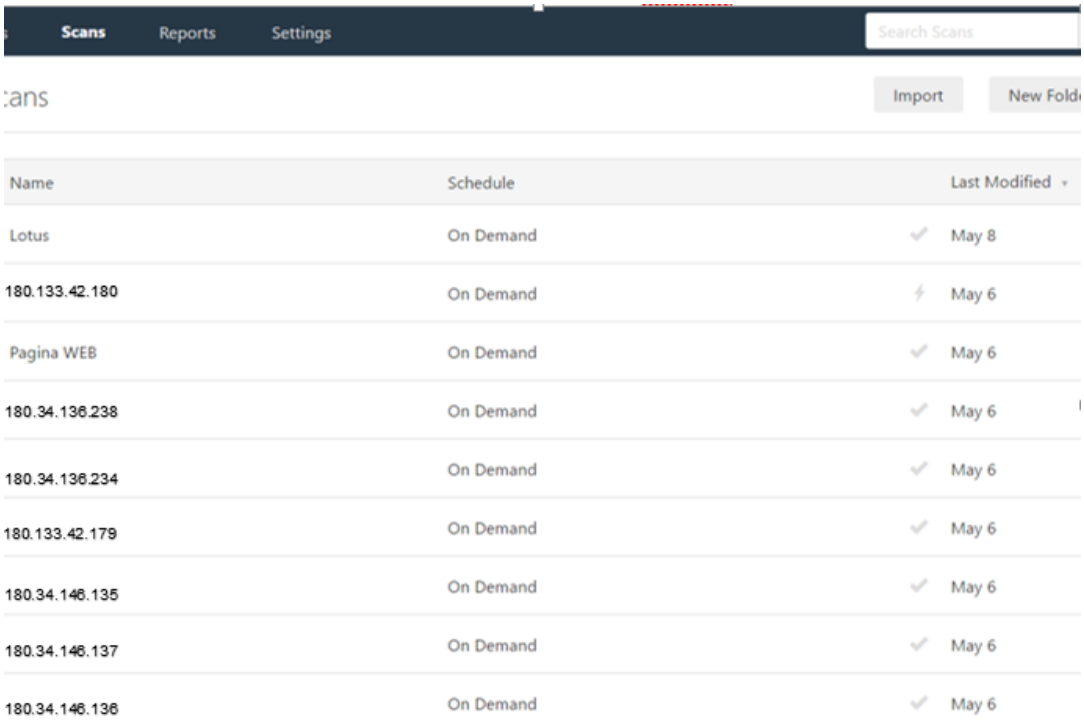
En los Anexos del documento se encuentran los informes de escaneos de la herramienta Nessus. Ver Anexos C Informes de Escaneos Nessus.

Ilustración 19. Opciones de escaneo herramienta Nessus



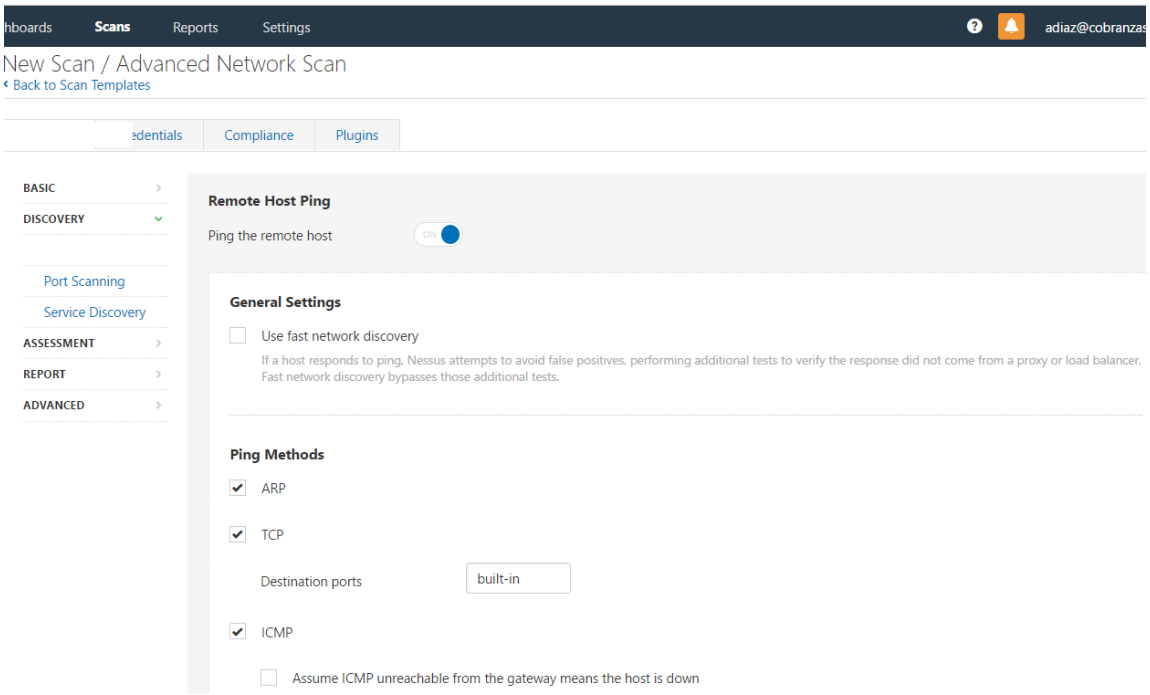
Fuente. Nessus opciones de escaneo. https://www.tenable.com/products/nessus-vulnerability-scanner.

Ilustración 20. Escaneos realizados con la plataforma de Nessus online



Fuente: Nessus. https://www.tenable.com/products/nessus-vulnerability-scanner.

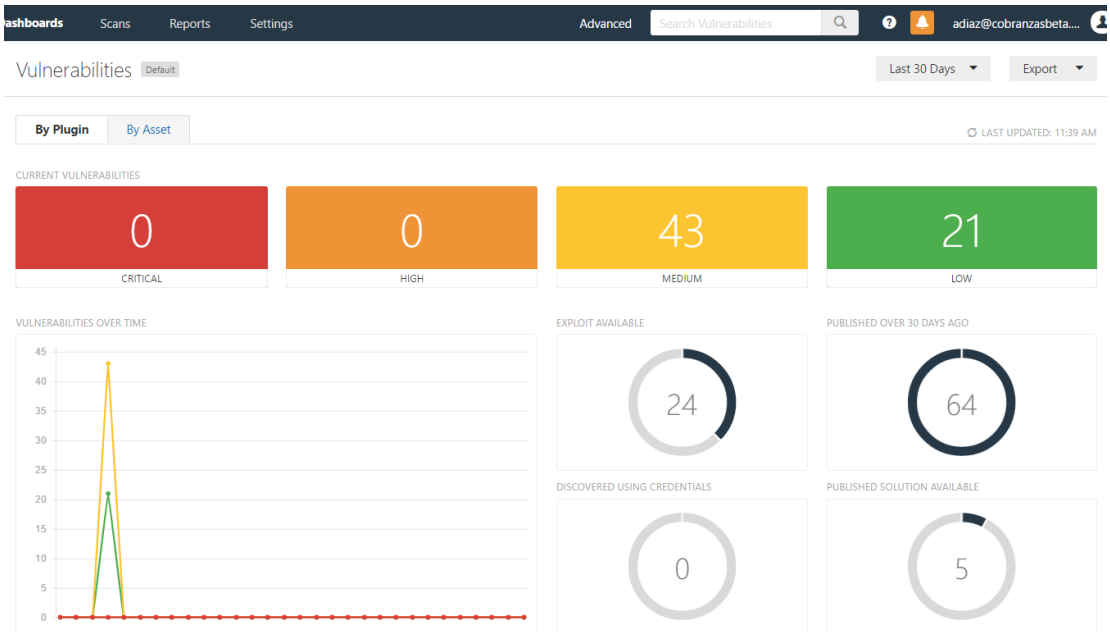
Ilustración 21. Parametrización de las opciones de escaneo programa Nessus



Fuente: Nessus. https://www.tenable.com/products/nessus-vulnerability-scanner

Al final de la actividad de escaneo de vulnerabilidades, se pueden generar varios tipos de informe, con el que la herramienta presenta un diagnóstico de las vulnerabilidades encontradas y describe la importancia de la vulnerabilidad en Crítica, Alta, Media y baja. Ver Ilustración 22.

Ilustración 22. Dashboard de las vulnerabilidades



Fuente: Nessus https://www.tenable.com/products/nessus-vulnerability-scanner.

En el informe de escaneo se describen más puntualmente las vulnerabilidades, relatando lo encontrado a detalle, el factor de riesgo, la referencia de información de la base de conocimiento de vulnerabilidades del Nessus, la posible solución, el activo vulnerable, y si es explotable la vulnerabilidad, con qué elementos se pudiera explotar, Ver Ilustración 23 Ejemplo de vulnerabilidad descrita por Nessus en el informe y ver Anexos C Informes de Escaneos Nessus.

Ilustración 23. Ejemplo de vulnerabilidad descrita por Nessus en el informe.

94437 (10) - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.8 (E:F/RL:ND/RC:ND)

References

CVE	CVE-2016-6329
CVE	CVE-2016-2183
BID	92631
BID	92630
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

190.24.137.118 (tcp/8443) Vulnerability State: Active

```
List of 64-bit block cipher suites supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
```

Fuente: https://www.tenable.com/products/nessus-vulnerability-scanner

En *Scan Report* se muestra el reporte completo generado por la herramienta Nmap de los puertos/servicios encontrados en las IP's públicas. Ver Ilustración 24. Reportes Herramienta Nmap.

Ilustración 24. Reportes Herramienta Nmap

Nmap Scan Report - Scanned at Sun Apr 30 13:14:20 2017

Scan Summary | ( )

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 13:14:20 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

- 180.133.42.180

Hostnames

-

Ports

The 991 ports scanned but not shown below are in state: **filtered**

Port		State (toggle closed [0] | filtered [0])	Service	Reason
25	tcp	open	smtp	syn-ack
80	tcp	open	http	syn-ack
110	tcp	open	pop3	syn-ack
143	tcp	open	imap	syn-ack
443	tcp	open	http	syn-ack
465	tcp	open	smtp	syn-ack
587	tcp	open	smtp	syn-ack
993	tcp	open	imap	syn-ack
995	tcp	open	pop3	syn-ack

Remote Operating System Detection

- Used port: **25/tcp (open)**
- OS match: **Linux 3.8 (91%)**
- OS match: **Linux 2.6.32 (90%)**
- OS match: **Linux 2.6.39 (90%)**
- OS match: **Linux 3.10 (89%)**
- OS match: **Linux 3.4 (89%)**
- OS match: **WatchGuard Fireware 11.8 (89%)**
- OS match: **Linux 3.1 - 3.2 (89%)**
- OS match: **Linux 2.6.32 or 3.10 (89%)**
- OS match: **Synology DiskStation Manager 5.1 (88%)**
- OS match: **Linux 2.6.32 - 2.6.39 (86%)**

Traceroute Information (click to expand)

- Traceroute data generated using port 587/tcp

Hop	Rtt	IP	Host
1	2.00	192.168.100.1	dtv.test
3	30.00	10.100.10.1	
5	110.00	10.100.10.10	
7	34.00	206.223.124.139	telmex-nap.ccit.org.co
8	35.00	181.49.179.138	
9	21.00	10.175.23.254	
10	22.00	190.144.32.186	
11	29.00		

Misc Metrics (click to expand)

Metric	Value
Ping Results	
System Uptime	484399 seconds (last reboot: Mon Apr 24 22:42:31 2017)
TCP Sequence Prediction	Difficulty=262 (Good luck!)
IP ID Sequence Generation	All zeros

Fuente: Nmap https://nmap.org/.

9.3.5 Vectores de Ataque. Teniendo en cuenta la definición brindada por la empresa de seguridad *Symantec**,*** un vector de ataque es el método que utiliza una amenaza para atacar un sistema, se realiza la revisión de los posibles métodos que un atacante puede utilizar para vulnerar los sistemas de la compañía, es así como llegamos al conocimiento de los vectores de ataque que pueden ser aprovechados por los delincuentes para sacar provecho de las vulnerabilidades.

9.3.5.1 Vectores de ataque al cifrado SSL. A continuación, se enumeran algunos de los ataques que se pueden realizar:

- Heartbleed: Es un error que se encuentra en las bibliotecas criptográficas OpenSSL. Este fallo les da la posibilidad a los cibercriminales de leer la información personal, consiguiendo con ello claves privadas y accesos a cuentas.
- POODLE: El problema está versiones antiguas del protocolo SSL, se remitía al uso de otras versiones TLS o de igual forma SSL obsoletas, con lo que se pueden optner datos guardados en cookies y descifrar información encriptada.
- FREAK: Permitía que se realizaran ataques men in the middle, dejando a los ciber-delincuentes en comunicación cuando se establece enlaces entre cliente y plataformas, consiguiendo así los datos interceptados. Es provocado por defectos en el software de OpenSSL.
- Shellshock: Afecta los usuarios permitiendo vulnerar el protocolo y permitiendo a los cibercriminales instalar malware’s y asimismo engañar a quienes visitan el sitio, con el fin de estafarlos o infectarlos. Si bien no es fallo de los certificados SSL, da muestra que para que SSL funcione correctamente debe de funcionar óptimamente el servidor.
- Bar Mitzvah: Esta vulnerabilidad corresponde a la intercepción de credenciales por el fallo del algoritmo encargado de la encriptación, el RC4. Según su uso corresponde al 30% de uso, algo que se busca cambiar pues ya existe la opción AES.

9.3.5.2 Vectores de ataque del correo electrónico y Rasomware. Mediante mensajes por correo electrónico, el usuario podría verse tentado a descargar archivos de dudosa procedencia o ingresar a links de descarga que permiten ejecutar aplicaciones de Rasomware, esto luego de análisis realizado con ingeniería social, haciendo que el delincuente juegue con las motivaciones y la curiosidad logrando que el usuario caiga en este tipo de ataques.

9.3.5.3 Vectores de Ataque páginas web. Este tipo de ataques suelen aprovechar vulnerabilidades conocidas en aplicaciones o servidores web, y normalmente tienen un fuerte impacto; para la validación de vectores de ataque, se toma como referencia el informe de “OWASP Top 10 Most Critical Web

Application Security Risks", dónde se definen los siguientes vectores de ataque que pueden ser utilizados por los ciber-delincuentes:

- Inyección.
- Autenticación y Gestión de Sesiones.
- Cross-Site Scripting (XSS).
- Control de Acceso roto.
- La configuración incorrecta de Seguridad.
- Sensible A6 Exposición de datos.
- Insuficiente Protección contra ataques.
- Cross-Site Request Falsificación.
- Utilización de componentes con vulnerabilidades conocidas.
- APIs subprotegidos (NUEVO).

9.3.6 Fase de Evaluación. En esta fase, se realiza la recopilación de los formatos de levantamiento de pentesting de los diferentes informes tomados de las herramientas usadas, para evaluar de manera técnica los resultados, los diagnósticos y los comentarios de la labor realizada en las actividades de la fase de escaneo, con esta información se ejecuta la evaluación de las vulnerabilidades, brindando un diagnóstico del estado de la seguridad de los servicios asociados a las IP's públicas de la compañía.

NOTA: Teniendo en cuenta que, dentro del alcance, sólo se realiza actividades de pentesting para la identificación de vulnerabilidades, sin que esto conlleve a aplicar fases de explotación de la vulnerabilidad, de acceso y de elevación de privilegios, dado que lo que se quiere evaluar es si es requerido incrementar las medidas de protección y generar recomendaciones que pudieran remediar las vulnerabilidades detectadas. Por lo tanto, si se requiere un nivel de evaluación más avanzado, se requeriría de una exploración de vulnerabilidades más integral, no solo ajustando a una porción, como es este caso de las IP's públicas donde él objetivo buscado es solo un diagnóstico de un escenario de ataque externo.

10. RESULTADOS

En este capítulo se definen los resultados obtenidos en el proceso de pentesting y el análisis de las vulnerabilidades, mostrando los hallazgos y exponiendo las actividades de remediación sugeridas o recomendadas.

En el proceso de ejecución de las distintas actividades expuestas en las fases de descubrimiento, planeación, escaneo y evaluación se pudo determinar un diagnóstico de seguridad informática a las IP's públicas de ASESORÍAS EN COBRANZAS MEGACOBRO y a sus servicios asociados, encontrando dentro de este ejercicio 64 hallazgos de vulnerabilidades las cuales tienen una criticidad media y baja, evidenciando que se han realizado algunos controles de seguridad, pero aún faltan controles más exhaustivos frente a servicios publicados.

Como se puede evidenciar en el Cuadro 1, se relacionan las vulnerabilidades, la descripción y la solución que se recomienda para mitigar el riesgo. Ver Cuadro 1. Descripción y solución de vulnerabilidades.

Cuadro 1. Descripción y solución de vulnerabilidades

Ítem	Hallazgos	Descripción	Solución	Ip
1	El servicio remoto admite el uso de cifrado de bloques de 64 bits	El host remoto admite el uso de un cifrado de bloque de 64 bits en una o más suites de cifrado, por lo tanto, está vulnerabilidad esta conocida con el nombre de SWEET32, debido a que el uso de un bloque de 64 bits es un cifrado débil, por lo tanto, un ataque de MIDM hombre-en-medio que tiene suficientes recursos puede Explotar esta vulnerabilidad. El uso de Cifrado de 64 bits es utilizado como en este hallazgo en el protocolo SSL en el cual se utiliza el cifrado 3DES cifrado que actualmente es vulnerable de ataque, en cambio cifrados como AES de bloques de 128, 256 y 512 son los más efectivos.	Se requiere reconfiguración de los servicios asociados a las IP´s encontradas con la vulnerabilidad, realizando el bloqueo de cifrado 3DES y adicionalmente limitando el número de peticiones a procesar sobre la misma conexión TLS.	180.34.127.218 y 180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
2	Algunos directorios en el servidor web remoto son navegables	Se encontró como vulnerabilidad sobre el sitio web de la compañía que varios directorios del sitio son navegables de forma directa y pueden permitir el acceso a información sensible.	Restringir la navegación de los directorios y solo mostrar por navegador la información necesaria, deshabilitar la indexación de directorios.	180.34.136.234
3	El servidor web remoto contiene un script PHP que es propenso a un ataque de divulgación de información	En muchas ocasiones en la instalación de servidores de PHP se realiza la prueba de configuración con la creación de un archivo phpinfo.php el cual puede ser de gran utilidad para los atacantes, ya que pueden obtener información de usuarios de instalación de PHP, la dirección IP del host, versión de sistema operativo, versión del servidor WEB, directorio raíz del servidor y la configuración que se tienen del servidor PHP	Eliminación del archivo phpinfo.php	180.34.136.234
4	El servidor web aloja archivos de SQL de acceso público	Se encontró en el servidor web archivos disponibles públicamente que contienen instrucciones SQL, los cuales pueden contener información de bases de datos que pueden ser confidenciales	Eliminar dichos archivos de SQL, para evitar que se acceda a ellos de forma remota y se atente con información confidencial.	180.34.136.234

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
5	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0, las cuales ya no son aceptables para comunicaciones seguras, dado que son vulnerables. Estos protocolos, sufren de varios defectos criptográficos y ha sido obsoleto durante varios años. Un atacante puede ser capaz de explotar estos problemas para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes.	Deshabilitar dentro de la aplicación los protocolos de cifrado SSl v2 y SSl V3.	180.133.42.180
6	Certificado SSL auto-firmado.	La cadena de certificados X.509 no está firmada por una autoridad de certificación reconocida; por lo tanto, cualquier persona podría establecer ataque de hombre-en-el medio contra el host o servicio publicado sobre la IP pública.	Se recomienda la compra o la generación de un certificado que garantice la seguridad del servicio publicado.	180.34.127.218 y 180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
7	El certificado SSl no es confiable.	No se puede confiar en el certificado X.509 del servidor, este evento se puede dar por: - la cadena de certificados enviada por el servidor puede no descender de un certificado público conocido o es un certificado auto firmado no reconocido, o cuando faltan certificados intermedios que conecten la parte superior de la cadena de certificados a un certificado público conocido. - La cadena de certificados puede contener un certificado que no es válido en el momento de la exploración esto puede ocurrir antes de una de las fechas del certificado o después de una de las fechas del certificado. - La cadena de certificados puede contener una firma que no coincide con la información del certificado o no puede ser verificada.	Se recomienda la compra o la generación de un certificado que garantice la seguridad del servicio publicado.	180.34.127.218 y 180.133.42.180
8	Cifrado SSL Compatible y de Mediana Fuerza	Al igual que en ítem 1 el host remoto admite el uso de cifrados SSL el cual está definido como cifrado de intensidad media, Nessus considera medio cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el 3DES.	Reconfigurar la aplicación afectada si es posible para evitar el uso de cifras de intensidad media.	180.34.127.218 y 180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
9	La aplicación Web potencialmente vulnerable a Clickjacking	El servidor web remoto no establece un encabezado de respuesta HTTP X-Frame o una directiva de contenido-seguridad 'frameancestors'. Esto podría potencialmente exponer el sitio a una clickjacking o interfaz de usuario, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable. Esto puede resultar en que un usuario realice transacciones en páginas fraudulentas o malintencionadas.	El encabezado de respuesta HTTP X-Frame-Options se puede utilizar para indicar si un navegador puede o no permitir presentar una página en un <frame> o <iframe>. Los sitios pueden usar esto para evitar los ataques de clickjacking, asegurando que su contenido no está incrustado en otros sitios, por lo tanto, se recomienda establecer la cabecera X-Frame-Options para todas las respuestas que contienen contenido HTML. Los valores posibles son "DENY", "SAMEORIGIN", o "PERMITIR-DE URL".	180.133.42.180
10	Certificado SSL con nombre de Host incorrecto	El certificado SSL de este servicio es para un host diferente, es decir, el commonName (CN) del certificado SSL presentado en este servicio es para una máquina diferente.	Se recomienda la compra o la generación de un certificado que garantice la seguridad del servicio publicado.	180.133.42.180
11	SSL / TLS EXPORT_RSA <= Complementos de cifrado de 512 bits compatibles (FREAK)	El host remoto admite conjuntos de cifrado EXPORT_RSA con claves inferiores o iguales a 512 bits. Un atacante puede factorizar un módulo RSA de 512 bits en un corto período de tiempo. Un atacante en el medio puede ser capaz de degradar la sesión para usar conjuntos de cifrado EXPORT_RSA (por ejemplo, CVE-2015-0204). Por lo tanto, se recomienda eliminar el soporte para conjuntos de cifrado débil.	Reconfigure el servicio para quitar la compatibilidad con los conjuntos de cifrado EXPORT_RSA.	180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
12	Certificado SSL firmado utilizando algoritmo de hash débil.	El servicio remoto asociado a la IP pública utiliza una cadena de certificados SSL que se ha firmado utilizando un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se disfrace como el servicio afectado. Tenga en cuenta que este complemento informa de todas las cadenas de certificados SSL firmadas con SHA-1 que caducaban después del 1 de enero de 2017 como vulnerables. Esto está de acuerdo con la gradual puesta a punto de Google del algoritmo de hash criptográfico SHA-1.	Se recomienda la compra o la generación de un certificado que garantice la seguridad del servicio publicado.	180.133.42.180
13	Divulgación de información de tipo man-in-the-middle (MitM) debido a un error en la implementación de AES-NI de OpenSSl	La implementación de AES-NI en OpenSSL antes de 1.0.1t y 1.0.2 antes de 1.0.2h no considera la asignación de memoria durante una comprobación de relleno determinada, lo que permite a atacantes remotos obtener información de texto claro sensible a través de un ataque de padding-oracle contra una sesión AES CBC. NOTA: esta vulnerabilidad existe debido a una corrección incorrecta para CVE-2013-0169.	Para corregir la Vulnerabilidad se recomienda actualizar a OpenSSL versión 1.0.1t / 1.0.2h o posterior.	180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
14	El servicio remoto admite el uso de cifrados SSL anónimos.	El host remoto admite el uso de cifrados SSL anónimos. Si bien esto permite a un administrador configurar un servicio que cifra el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar el control remoto La identidad del anfitrión y hace que el servicio sea vulnerable a un ataque de man-in-the-middle. Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.	Se recomienda reconfigurar la aplicación afectada para evitar el uso de cifras débiles y certificados anónimos.	180.133.42.180

15	El servidor de correo permite login SMTP de sesión en texto Plano	El host remoto asociado a la IP pública está ejecutando un servidor SMTP que permite conexiones de texto sin cifrado sobre conexiones no cifradas. Un atacante puede ser capaz de descubrir nombres de usuario y contraseñas escaneando el tráfico al servidor, se está utilizando un mecanismo de autenticación inseguro (es decir, LOGIN o PLAIN).	Se requiere que se configure el servicio para que admita mecanismos de autenticación seguros únicamente a través de un canal cifrado.	180.133.42.180
16	Login de sesión de POP3 en texto Plano.	El host remoto está ejecutando un daemon POP3 que permite conexiones de texto sin cifrado sobre conexiones no cifradas. Un atacante puede descubrir nombres de usuario y contraseñas al escanear el tráfico al daemon POP3	Se recomienda realizar cifrado de tráfico con SSL / TLS utilizando stunnel.	180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip
17	El servicio remoto admite el uso del cifrado RC4.	El algoritmo RC4, tal como se utiliza en el protocolo TLS y el protocolo SSL, tiene muchos sesgos de un solo byte, lo que facilita a los atacantes remotos realizar ataques de recuperación de texto sin cifrar mediante un análisis estadístico del texto cifrado en un gran número de sesiones que usan el mismo texto claro.	Reconfigurar la aplicación afectada, si es posible, para evitar el uso de cifras RC4. Considerar la posibilidad de utilizar TLS 1.2 con las suites AES-GCM sujetas al soporte de navegador y servidor web.	180.133.42.180

18	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman inferiores o iguales a 1024 bits.	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman inferiores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede ser capaz de encontrar el secreto compartido en un corto período de tiempo (dependiendo del tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.	Para mitigar esta vulnerabilidad se recomienda reconfigurar el servicio para que utilice módulos Diffie-Hellman únicos de 2048 bits o más.	180.133.42.180
19	SSL / TLS EXPORT_DHE <= 512 bits, exportación de cifrado Suites compatibles	El host remoto admite conjuntos de cifrado EXPORT_DHE con claves inferiores o iguales a 512 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en un corto período de tiempo. Un atacante en el medio puede rebajar la sesión para usar los conjuntos de cifrado EXPORT_DHE. Por lo tanto, se recomienda eliminar el soporte para conjuntos de cifrado débil.	Se recomienda reconfigurar el servicio asociado a la IP pública para quitar la compatibilidad con los conjuntos de cifrado EXPORT_DHE.	180.133.42.180

Cuadro 1. (Continuación)

Ítem	Hallazgos	Descripción	Solución	Ip

20	El servidor web remoto puede transmitir las credenciales en texto sin cifrar.	El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'contraseña' que transmiten su información a un servidor web remoto en texto sin cifrar. Un atacante que escuche el tráfico entre el navegador web y el servidor puede obtener inicios de sesión y contraseñas de usuarios válidos.	Se recomienda que se transmita contenido a través de HTTPS, como una forma segura de comunicación.	180.34.136.234

Fuente: Diseñadores del proyecto

La descripción y soluciones expuestas en el cuadro 1 se tomó en base a la documentación adquirida en la herramienta de análisis de vulnerabilidad y en informes de seguridad informática que evidencian la criticidad de los hallazgos y cómo la compañía debe afrontarlos para mitigar los riesgos y evitar así posibles pérdidas económicas o reputacionales.

Los informes consultados y de referencia para la documentación de los hallazgos son:

- OWASP Top 10 -2013 y OWASP Top 10 2017 de los 10 riesgos más críticos en Aplicaciones; entre ellos los riesgos del cifrado no seguro. https://www.owasp.org/index.php/Testing_for_SSL-TLS_ (OWASP-CM-001).
- Internet Security Threar Report ISTR de Symantec de abril de 2017 donde se evidencia el uso de certificados de seguridad y los riesgos de no tener estas prácticas que pueden ser usadas por atacantes para vulnerar la información.
- Informe Anual de Seguridad Cisco 2016 donde se puede ver los casos de seguridad más vulnerables y la tendencia de uso de protocolos de cifrado para protección de información.
- UIT Unión internacional de Telecomunicaciones Guía Marco de Autenticación X509 The SWEET32 Issue, CVE-2016-2183.
- https://www.openssl.org/blog/blog/2016/08/24/sweet32/.
- Clickjacking Defense Cheat Sheet.
- https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet.
- (CVE-2014-3571) https://www.openssl.org/news/secadv/20150108.txt.
- CVE-2015-0204 Detail - https://nvd.nist.gov/vuln/detail/CVE-2015-0204.
- CVE-2004-2761 Detail - https://nvd.nist.gov/vuln/detail/CVE-2004-2761.
- CVE-2016-2107 Detail - https://nvd.nist.gov/vuln/detail/CVE-2016-2107.
- CVE-2013-2566 Detail - https://nvd.nist.gov/vuln/detail/CVE-2013-2566.

- https://tools.ietf.org/html/rfc4422

10.1 DIAGNÓSTICO DE SEGURIDAD

Aunque se pudo establecer que las configuraciones de algunos servicios publicados en internet bajo las IP´s públicas escaneadas, evidencian tener en su configuración vulnerabilidades que pueden ser explotadas por atacantes externos, sin embargo, teniendo en cuenta el informe de la herramienta de escáner de vulnerabilidad Nessus, estas solo hacen referencia a vulnerabilidades catalogadas como medias y bajas, por lo que también se puede establecer que la compañía cuenta con un nivel mínimo de controles de seguridad que evitan que las vulnerabilidades pasen a ser críticas y expongan del todo la información de la compañía.

Es por esto, que en su mayoría las vulnerabilidades detectadas hacen referencia a problemas con los métodos de cifrado, autenticación y protocolos SSL en versiones antiguas que son vulnerables.

De igual manera, pero en menor medida se detectaron fallas en las configuraciones de los servicios, como, por ejemplo, la no eliminación de archivos de prueba de configuración como el infophp.php o archivos de scripts de SQL, y algunos errores de configuración de permisos para la no visualización los directorios de los servidores web, los cuales pueden permitir la posible divulgación de información a los atacantes.

Por último, aunque en este ejercicio las actividades de remediación hacen referencia a configuraciones propias de los protocolos de cifrado, cambio de permisos y la recomendación de compra de certificados de seguridad emitidos por empresas certificadoras, no hay que dejar de lado aspectos tan importantes como los controles en los procesos de calidad y aseguramiento de servicios y servidores a producción por medio de Hardering , se recomienda también, una continua revisión de procesos de testing interno y externo de las aplicaciones de forma más general y exhaustiva en comparación del ejercicio realizado y plasmado en este documento, ya que este, solo evidencia una porción de un gran objetivo que es asegurar la información.

También, se hace necesario resaltar la importancia de las capacitaciones a los funcionarios en ingeniería social, teniendo en cuenta, que el recurso humano es el eslabón más débil o más fuerte según su conocimiento de los ataques que los delincuentes informáticos realizan constantemente para vulnerar tanto la información como las plataformas propias de la compañía.

10.2 GESTIÓN DE VULNERABILIDADES

Para ayudar a la evaluación y priorización de las vulnerabilidades encontradas en las herramientas, se procedió a realizar la comparación de las vulnerabilidades con el puntaje CVSS.

Este sistema de puntaje está diseñado para ser un estándar abierto, que colabore en la tarea de estimar el impacto derivado de las vulnerabilidades, es decir, cuantificar de alguna manera la severidad de las vulnerabilidades.

Este método se calcula en una escala que va del 0 al 10. La severidad se considera baja si el puntaje obtenido luego de aplicar la fórmula CVSS resulta entre 0.0 y 3.9. El impacto es medio si el resultado se ubica entre 4.0 y 6.9. Se considera alto cuando el puntaje cae dentro del rango 7.0 y 10.0[16].

Para realizar el cálculo del puntaje, este esquema se basa en tres grupos de métricas que son Métricas Base, Métricas Temporales y Métricas de Entorno.

10.2.1 Métricas Base:

De este grupo hace parte características intrínsecas a la vulnerabilidad y apuntan al entorno del usuario, además, intenta determinar los impactos de manera independiente, en cuanto a Confidencialidad, Integridad y Disponibilidad.

10.2.2 Métricas Temporales:

Son aquellas características de la vulnerabilidad que puede cambiar en el tiempo, se tienen en cuenta: - explotabilidad, - nivel de remediación – reporte de confianza.

10.2.3 Métricas de Entorno:

Representan características de una vulnerabilidad asociadas sobre todo al entorno de usuario, incluye: - daño potencial, - colateral, y – distribución de objetivos.

Dentro de este proyecto, no se hallaron métricas de entorno, sin embargo, en todas existen métricas base y sólo 6 de las 20 tomadas como muestra, se encuentran con métricas temporales.

En las métricas base los datos evaluados son:

- Vector de Ataque (AV): red (AV: N), red adyacente (AV: A), local (AV: L), física (AV: P).

[16] MENDOZA, Miguel Ángel. Vulnerabilidades ¿Qué es CVSS y cómo utilizarlo? 4 de agosto de 2014. Disponible en internet: https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

- Ataque de Complejidad (AC): baja (AC: L), alta (AC: H).
- Privilegio Necesarios (PR): ninguno (PR: N), bajo (PR: L), alta (PR: H).
- Interacción de usuario (AU): ninguno (UI: N), obligatorio (UI: R).
- Alcance (S): sin cambios (S: U), con cambios (S: C).
- Impacto confidencialidad (C): ninguno (C: N), bajo (C: L), alta (C: H).
- Impacto de integridad (I): ninguno (I: N), bajo (I: L), alta (I: H).
- Impacto de disponibilidad (D): ninguno (A: N), bajo (A: L), alta (A: H).

Las métricas temporales son:

- Explotabilidad (E): no definido (E: X), no demostrada de que existe explotación (E: T), prueba de concepto (E:P), funcional exploit (E: F), alto (E: H).
- Nivel de remediación (RL): oficial (RL: O), arreglo temporal (RL: T), solución (RL: W), no disponible (RL: U).
- Informe de confianza (RC): no definido (RC: X), desconocido (RC: U), razonable (RC: R), confirmado (RC: C).

En el Cuadro 2, se hace un desglose del puntaje CVSS por vulnerabilidad e IP's. Ver Cuadro 2. Desglose CVSS.

Cuadro 2. Desglose CVSS

Ítem	Hallazgos	CVSS	Ip
1	El servicio remoto admite el uso de cifrado de bloques de 64 bits	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado. **Temporal Score:** 4.8 (E: F/RL:ND/RC:ND) El puntaje indica un impacto medio. A nivel de explotabilidad existe código que puede funcionar en la mayoría de situaciones en las que existe la vulnerabilidad, se puede saltar la métrica de informe de confianza.	180.34.127.218 y 180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
2	Algunos directorios en el servidor web remoto son navegables	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado.	180.34.136.234
3	El servidor web remoto contiene un script PHP que es propenso a un ataque de divulgación de información	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado.	180.34.136.234
4	El servidor web aloja archivos de SQL de acceso público	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado.	180.34.136.234

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
5	El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado.	180.133.42.180
6	Certificado SSL auto-firmado.	**Base Score:** 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario, puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, puede también haber perdida completa de la protección y el atacante podría cambiar los datos, no hay impacto a disponibilidad del componente atacado.	180.34.127.218 y 180.133.42.180
7	El certificado SSl no es confiable.	**Base Score:** 6.4 (AV:N/AC:L/Au:N/C:P/I:P/D:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario, puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, puede también haber perdida completa de la protección y el atacante podría cambiar los datos, no hay impacto a disponibilidad del componente atacado.	180.34.127.218 y 180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
8	Cifrado SSL Compatible y de Mediana Fuerza	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, a nivel de complejidad un atacante puede esperar el éxito repetible contra el componente atacado, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, sin embargo, no hay impacto a la integridad ni a la disponibilidad del componente atacado.	180.34.127.218 y 180.133.42.180
9	La aplicación Web potencialmente vulnerable a Clickjacking	**Base Score:** 4.3 (AV:N/AC:H/Au:N/C:N/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; No puede haber una pérdida de la confidencialidad, pero si se podría perder control de la protección y el atacante tendría acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180
10	Certificado SSL con nombre de Host incorrecto	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad no necesita condiciones especiales, puede vulnerarse sin la interacción del usuario; No puede haber una pérdida de la confidencialidad, pero si se podría perder control de la protección y el atacante tendría acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
11	SSL / TLS EXPORT_RSA <= Complementos de cifrado de 512 bits compatibles (FREAK)	**Base Score:** 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad no necesita condiciones especiales, puede vulnerarse sin la interacción del usuario; No puede haber una pérdida de la confidencialidad, pero si se podría perder control de la protección y el atacante tendría acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado. **Temporal Score:** 4.1 (E:F/RL:OF/RC:ND) El puntaje indica un impacto medio. En la probabilidad de explotación existe un código que puede ser funcional en situaciones donde exista esta vulnerabilidad, existe una actualización o parche oficial disponible y se puede saltar la métrica del informe de confianza.	180.133.42.180
12	Certificado SSL firmado utilizando algoritmo de hash débil.	**Base Score:** 4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante y se podría perder control de la protección y el atacante tendría acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado. **Temporal Score:** 3.5 (E:ND/RL:OF/RC:C) El puntaje indica un impacto medio. En la probabilidad de explotación se puede omitir esta métrica, existe una actualización o parche oficial disponible y existen informes detallados y código de exploits funcionales disponibles para verificar la vulnerabilidad.	180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
13	Divulgación de información de tipo man-in-the-middle (MitM) debido a un error en la implementación de AES-NI de OpenSSl	**Base Score:** 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180
14	El servicio remoto admite el uso de cifrados SSL anónimos.	**Base Score:** 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado. **Temporal Score:** 2.3 (E:ND/RL:OF/RC:C) El puntaje indica un impacto bajo. En la probabilidad de explotación se puede omitir esta métrica, existe una actualización o parche oficial disponible y existen informes detallados y código de exploits funcionales disponibles para verificar la vulnerabilidad.	180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
15	El servidor de correo permite login SMTP de sesión en texto Plano	**Base Score:** 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180
16	Login de sesión de POP3 en texto Plano.	**Base Score**: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
17	El servicio remoto admite el uso del cifrado RC4.	**Base Score**: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado. **Temporal Score:** 2.2 (E:F/RL:TF/RC:ND) El puntaje indica un impacto bajo. En la probabilidad de explotación existe condigo funcional que funciona en las situaciones donde existe la vulnerabilidad, hay una solución oficial o temporalmente disponible para tratar la vulnerabilidad y se puede omitir la métrica de informe de confianza.	180.133.42.180
18	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman inferiores o iguales a 1024 bits.	**Base Score:** 2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; no puede haber una pérdida total de la confidencialidad, pero se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.133.42.180

Cuadro 2. (Continuación)

Ítem	Hallazgos	CVSS	Ip
19	SSL / TLS EXPORT_DHE <= 512 bits, exportación de cifrado Suites compatibles	**Base Score:** 2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; no puede haber una pérdida total de la confidencialidad, pero se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado. **Temporal Score:** 2.2 (E:F/RL:TF/RC:ND) El puntaje indica un impacto bajo. En la probabilidad de explotación existe condigo funcional que funciona en las situaciones donde existe la vulnerabilidad, hay una solución oficial o temporalmente disponible para tratar la vulnerabilidad y se puede omitir la métrica de informe de confianza.	180.133.42.180
20	El servidor web remoto puede transmitir las credenciales en texto sin cifrar.	**Base Score**: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N) El puntaje indica un impacto medio. Es una vulnerabilidad explotable con acceso a la red, nivel de complejidad necesita de un atacante preparado y el éxito depende de las condiciones, puede vulnerarse sin la interacción del usuario; puede haber una pérdida total de la confidencialidad, lo que significa que los componentes divulguen información al atacante, pero no se podría perder control de la protección para que el atacante tenga acceso a modificación de datos, no hay impacto a la disponibilidad del componente atacado.	180.34.136.234

Fuente: Diseñadores del proyecto

10.3 Impactos para la Compañía

Los datos de la compañía son el activo más valioso, dado que en ellos se encuentra el insumo para realizar las operaciones diarias y los procesos que se requieren para desarrollar la actividad económica, además no hay que olvidar que los datos personales de los clientes hay que resguardarlos en mayor medida y es por esto que la seguridad informática es tan importante y debe velar por mitigar los riesgos y las vulnerabilidades identificadas, ya que al no tener una buena práctica de asegurar la información y mitigar los riesgos producto de las vulnerabilidades que se tengan la compañía se expone a perdidas tanto económicas, perdida de reputación en el mercado y las sanciones legales que pueden ocasionarse por perdidas de información, producto de los ataques informáticos.

10.3.1 Sanciones Legales.

Dentro de la legislación colombiana hay que tener en cuenta las posibles sanciones que se pueden obtener por divulgación de datos personales, los cuales pueden ser sancionados por La Superintendencia de Industria y Comercio en un eventual suceso de perdida de información y divulgación de bases de clientes. Por ejemplo, por una violación a la Ley 1581 la sanción pude llegar a los 2000 SMMLV (Salario Mínimo Mensuales Legales Vigentes), sumado a esto se puede también, tomar medidas de suspensión de actividades, cierre parcial o definitivo de la compañía.

10.3.2 Perdidas Reputaciones.

La materialización de los riesgos por causa de eventos de seguridad informática exponen a la empresa, no solo a pérdidas económicas, o sanciones legales, sino también a perdidas reputaciones las cuales pueden ser más serias, ya que atenta con la competitividad en el mercado, la satisfacción de los clientes por los servicios ofrecidos, la fluidez y fidelización de los mismos, entre otros factores, los cuales pueden atentar aún más con el hecho de perder la información de la compañía por un evento de hacker o de delincuencia informática.

10.3.3 Pérdidas Económicas.

Los ataques informáticos en el mundo dejan millones de dólares en pérdidas para las compañías cada año, información de clientes, vulneraciones a los sistema que aumentan día a día debido a las vulnerabilidades presentes y las cuales no son mitigadas y aprovechadas por los delincuentes; según el estudio realizado por Fortinet del panorama de la seguridad informática en Colombia, se encontró que más del 80 por ciento de las compañías en el país poseen sistemas altamente vulnerables, y estos pueden representar al país una gran cantidad de dinero en pérdidas económicas.

10.3.4 De igual manera los costos asociados al cibercrimen de acuerdo con una encuesta sobre el Estado Global de Seguridad[17] de la Información publicada por Price Water House Cooper, el impacto económico global se estimó en US$ 575.000 millones en 2015, donde América Latina y el Caribe sumaron costos por US$ 90.000 millones anuales, representando el 16% del costo total mundial del delito y cuatro veces más que la inversión social internacional. (Espectador 27 de octubre de 2016)

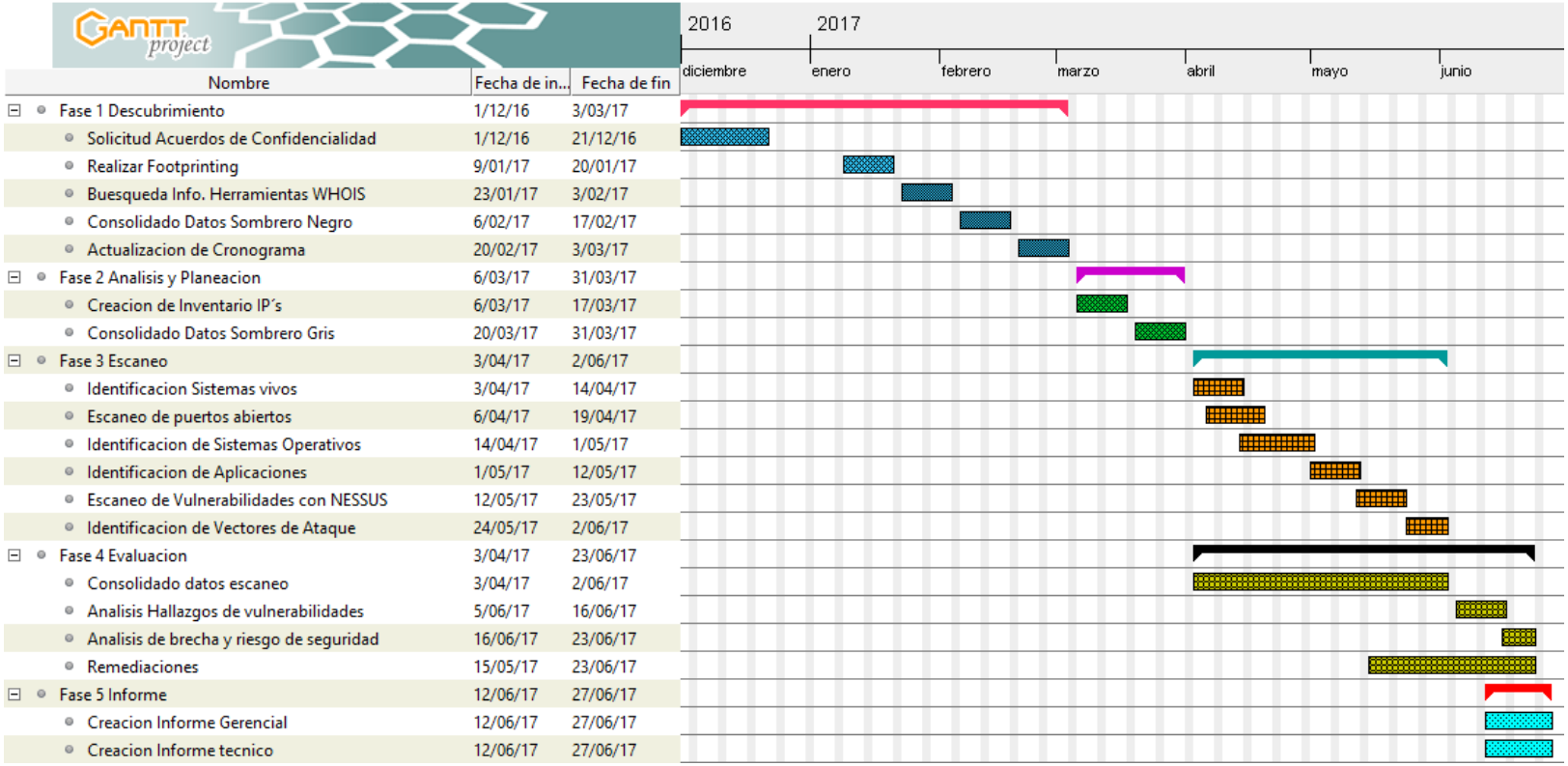
En el caso particular del riesgo económico está asociado a las posibles multas que un evento de robo de información de clientes puede ocasionar los cuales pueden estar asociados a sanciones de la Superintendencia de Industria y Comercio, por mal manejo de datos personales de clientes, a su vez, estos conllevan a daños reputaciones que desvirtúan la fidelidad de los clientes y pueden afectar el mercado de la compañía.

[17] PRICE WATER HOUSE COOPER. Crear Confianza en el Mundo Digital. 2015. Disponible en: http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf

11. **CRONOGRAMA**

Para la ejecución del proyecto se realiza un cronograma de actividades. Ver ilustración 25. Cronograma del proyecto.

Ilustración 25. Cronograma del proyecto.



Nombre	Fecha de in...	Fecha de fin
Fase 1 Descubrimiento	1/12/16	3/03/17
Solicitud Acuerdos de Confidencialidad	1/12/16	21/12/16
Realizar Footprinting	9/01/17	20/01/17
Buesqueda Info. Herramientas WHOIS	23/01/17	3/02/17
Consolidado Datos Sombrero Negro	6/02/17	17/02/17
Actualizacion de Cronograma	20/02/17	3/03/17
Fase 2 Analisis y Planeacion	6/03/17	31/03/17
Creacion de Inventario IP´s	6/03/17	17/03/17
Consolidado Datos Sombrero Gris	20/03/17	31/03/17
Fase 3 Escaneo	3/04/17	2/06/17
Identificacion Sistemas vivos	3/04/17	14/04/17
Escaneo de puertos abiertos	6/04/17	19/04/17
Identificacion de Sistemas Operativos	14/04/17	1/05/17
Identificacion de Aplicaciones	1/05/17	12/05/17
Escaneo de Vulnerabilidades con NESSUS	12/05/17	23/05/17
Identificacion de Vectores de Ataque	24/05/17	2/06/17
Fase 4 Evaluacion	3/04/17	23/06/17
Consolidado datos escaneo	3/04/17	2/06/17
Analisis Hallazgos de vulnerabilidades	5/06/17	16/06/17
Analisis de brecha y riesgo de seguridad	16/06/17	23/06/17
Remediaciones	15/05/17	23/06/17
Fase 5 Informe	12/06/17	27/06/17
Creacion Informe Gerencial	12/06/17	27/06/17
Creacion Informe tecnico	12/06/17	27/06/17

Fuente: Diseñadores del proyecto.

12. CONCLUSIONES

- Se logró establecer un cronograma con los tiempos y desglose de tareas, que permitió mostrar a la empresa el plan de trabajo y el desarrollo del proyecto, el cual se cumplió según la proyección.

- El Pentesting desarrollado para la búsqueda de vulnerabilidades a los servicios asociados a las IP´s públicas de la compañía, sólo es un proceso inicial de diagnóstico de la seguridad informática que se puede realizar, ya que solo se ha escaneado una pequeña porción de los sistemas de comunicación e información orientados a lo expuesto en Internet; para poder tener una verdadera percepción de seguridad, se deben realizar procesos más elaborados y exhaustivos de todos los activos de la información, evaluando los riesgos y los controles asociados para mitigarlos.

- En este proceso de búsqueda y análisis de vulnerabilidades se logró constatar que existen vulnerabilidades que pueden afectar la información de la compañía, ocasionado por la exposición a Internet y a posibles ataques informáticos, por tal motivo, se deben tener en cuenta las remediaciones sugeridas para mitigar los riesgos y realizar periódicamente análisis o escaneos de vulnerabilidades para proteger a la organización de mejor manera.

- Por último, aunque en este ejercicio las actividades de remediación hacen referencia a configuraciones propias de los protocolos de cifrado, cambio de permisos y la recomendación de compra de certificados de seguridad emitidos por empresas certificadoras, no hay que dejar de lado aspectos tan importantes como los controles en los procesos de calidad y aseguramiento de servicios y servidores a producción por medio de Hardering, la continua revisión de procesos de testing interno y externo de las aplicaciones de una forma más general y exhaustiva en comparación del ejercicio realizado y plasmado en este documento, el cual sólo evidencia una porción de un gran objetivo que es asegurar la información.

- Cada conclusión de este documento se dará a conocer a la compañía con el fin de que tenga un conocimiento completo de lo realizado, y sujete a evaluación la aprobación y ejecución de las recomendaciones sugeridas.

Sin embargo, no se puede dejar a un lado la importancia de las capacitaciones a los funcionarios en ingeniería social, el cual puede ser el eslabón más débil o más fuerte, según el conocimiento de los ataques

que los delincuentes informáticos pueden realizar para afectar la información como las plataformas propias de la compañía.

13. REMEDIACIONES SUGERIDAS

En consideración de los hallazgos se concluyó que las remediaciones más adecuadas para mitigar los riesgos asociados a las vulnerabilidades encontradas son:

- Adquisición de certificados de seguridad SSL/TLS a autoridades certificadoras por parte de la Empresa para garantizar que se mitigue la vulnerabilidad asociada a las aplicaciones que tienen hallazgos al uso de certificados desconocidos, auto-firmados, obsoletos y/o no válidos.

- Se recomienda la adquisición, instalación y configuración de estos certificados digitales a los servicios web asociados a las IP´s públicas, para autenticar y cifrar la información de una manera segura y confiable.

- Realizar la revisión general de las configuraciones de los servicios y comunicaciones que realicen uso de cifrado débil y quitar de las configuraciones Algoritmos criptográficos vulnerables como DES, 3DES, Diffie-Helman, algoritmos de hash como SHA y SHA1 e implementar métodos de cifrado más robusto.

- Implementar un proceso de hardering exhaustivo para los servidores y servicios publicados, teniendo en cuenta los puertos necesarios para los servicios, el cifrado, los certificados de seguridad, los medios de autenticación e intentos simultáneos, las configuraciones de los servicios web para evitar ataques de DDoS, phishing, Inyección de SQL, e implementar sistemas de protección contra ataques de fuerza bruta, como Fail2ban o cualquier otro software de vaneo de IP por intentos de autenticación no válidos.

- Implementar un proceso de Pentesting o búsqueda de vulnerabilidades periódico para descubrir posibles riesgos que deban ser mitigados y así generar mayor seguridad a la información y activos de la compañía.

ANEXO A

Formato de Levantamiento Pentesting

Formato de levantamiento Pentesting					
Fecha:					
Nombre:			# de ID		
Fase de Busqueda					
IP:	MASk				
Puertos	Servicios Asociados	URL			
Comentarios					
Diagnostico					
Herramientas Usadas					
Nombre herramienta	Descripcion				
Firmas de Aceptacion					
Alexander Diaz Pulido			Marcela Ramirez		

[18]

[18] Fuente Propia

Formato de levantamiento Pentesting					
Fecha:	11/05/2017				
Nombre:	Alexander Diaz Pulido		# de ID	1	
Fase de Busqued.					
IP:	MASk				

Puertos	Servicios Asociados	URL	A-Externo
21	FTP	:21	OFF
8008	EFA (Email Filter)(TCP)	N/A	ON
4443	EFA (Email Filter)(TCP)	:4443	ON

Comentarios
Para el servicio FTP en NAT a un servidor Interno, con restriccion de acceso a direcciones IP Externas, configurado desde El firewall. En el caso de el servicio EFA, la herramienta Nmap encontro puertos asociados que permiten acceso via web a servicio.

Diagnostico
Se realiza escaneo de la Ip publica desde las herramientas Nmap y Nessus para identificar posibles vulnerabilidades pero estas herramientas no lograron llegar al servicio de la FTP debido a la restriccion de acceso configurado en el servicio Firewall de la compañia. Para el servicio EFA(Mail Filter) la herramientas Nmap Logro Identificar dos puertos de su funcionamiento y se pudo identificar que puede ser accedido via web a uno de ello; se pudo establecer tambien que por configuracion de complejidad de contraseña y de intentos de logueo el sistema puede banear los intentos no autorizados ocacionados por posibles ataques de fuerza bruta, limitando asi las posiblidades de ataques externos. La herramienta nessus no identifico Vulnerabilidades dentro de su proceso de diagnostico.

Herramientas Usadas	
Nombre herramienta	Descripcion
NMAP	Se realiza escaner con ping y sin ping directamente a las direcciones y no encuentra activo host se usan los comandos: nmap -T4 -A -v y nmap -T4 -A -v -Pn
NESSUS	nessus y la herramienta no encuentra vulnerabilidad alguna en la configuracion y servicios asociados a esta ip.

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

19

[19] Fuente Propia IP: 180.133.42.176

Formato de levantamiento Pentesting						
Fecha:	11/05/2017					
Nombre:	Alexander Diaz Pulido		# de ID			
Fase de Busqued						
IP:	MASk					

Puertos	Servicios Asociados	URL	A-Externo
443	SSL/HTTP (TCP)		off
80	HTTP (TCP)		off
22	SSH (TCP)		off
10000	HTTP/Webmin (TCP,UDP		off
995	Desconocido (UDP)		off
5060	SIP-PROXY (UDP)		off
17331	Desconocido (UDP)		off
19995	Desconocido (UDP)		off

Comentarios
Existen servicios asociados a un servidor de Voz IP con los puertos TCP y UDP pero se encuentran limitado su acceso a direcciones permitidas por Firewall y por configuracion de iptables del servidor, por lo tanto, al realizar el escaneo de la ip publica las herramientas nmap, wireshark y Nesssus no encontraron dispositivos asociados o activos en la ip publica.

Diagnostico
Por encontrarse configurado en los sistemas de Firewall y internamente en el servidor accesos por Iptables no fue posible identificar servicios asociados a la ip publica de manera externa, esto garantiza que para un atacante la no se evidencie servicios que puedan ser vulnerados.

Herramientas Usadas	
Nombre herramienta	Descripcion
NMAP	La herramienta NMAP no genera informacion realizando el escaneo a la ip publica, se realizan escaneos con ping, sin ping, udp y tcp a todos los puertos.
WIRESHARK	El wiresharck no evidencia equipo activo luego de validar existencia por medio de trafico y comandos ping a esta direccion y la bandera del ICMP esta en
NESSUS	El sistema nessus no encuentra vulnerabilidades luego de realizar el diagnostico a la direccion IP.

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

20

[20] Fuente Propia IP: 180.133.42.177

Formato de levantamiento Pentesting						
Fecha:	11/05/2017					
Nombre:			# de ID			
Fase de Busqued						
IP:	MASk					

Puertos	Servicios Asociados	URL	A-Externo
443	SSL/HTTP (TCP)		off
80	HTTP (TCP)		off
22	SSH (TCP)		off
10000	HTTP/Webmin (TCP,UDP		off
995	Desconocido (UDP)		off
5060	SIP-PROXY (UDP)		off
17331	Desconocido (UDP)		off
19995	Desconocido (UDP)		off

Comentarios
Al igul que la IP 187 Existen servicios asociados a un servidor de Voz IP con los puertos TCP y UDP pero se encuentran limitado su acceso a direcciones permitidas por Firewall y por configuracion de iptables del servidor, por lo tanto, al realizar el escaneo de la ip publica las herramientas nmap, wireshark y Nesssus no encontraron dispositivos asociados o activos e la ip publica.

Diagnostico
Por encontrarse configurado en los sistemas de Firewall y internamente en el servidor accesos por Iptables no fue posible identificar servicios asociados a la ip publica de manera externa, esto garantiza que para un atacante la no se evidencie servicios que puedan ser vulnerados

Herramientas Usadas	
Nombre herramienta	Descripcion
NMAP	La herramienta NMAP no genera informacion realizando el escaneo a la ip publica, se realizan escaneos con ping, sin ping, udp y tcp a todos los
WIRESHARK	El wiresharck no evidencia equipo activo luego de validar existencia por medio de trafico y comandos ping a esta direccion y la bandera del ICMP.
NESSUS	El sistema nessus no encuentra vulnerabilidades luego de realizar el diagnostico a la direccion IP.

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

21

[21] Fuente Propia IP: 180.133.42.178

Formato de levantamiento Pentesting					
Fecha:					
Nombre:			# de ID		
Fase de Busquec					
IP:	MASk				
Puertos	Servicios Asociados	URL			

Comentarios
No se encuentra a la fecha Servicio Asociado a esta ip.

Diagnostico

Herramientas Usadas	
Nombre herramienta	Descripcion

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

22

[22] Fuente Propia IP: 180.133.42.179

Formato de levantamiento Pentesting				
Fecha:				
Nombre:			# de ID	
Fase de Busqued				
IP:	MASk			

Puertos	Servicios Asociados	URL	A-Externo
25	SMTP (TSP)		ON
80	HTTP (TSP)		ON
110	POP3 (TSP)		ON
143	IMAP(TSP)		ON
465	SMTP (TSP)		ON
587	SSL/SMTP (TSP)		ON
993	SSL/IMAP (TSP)		ON
995	SSL/POP3 (TSP)		ON

Comentarios
Se encuentra en la direccion 190.24.136.190 el alojamiento del correo Zimbra con dominio .com.co, el cual presenta los puertos de conexión al correo (http) y los necesarios para la configuracion de entrada y salida de correos (imap, smtp, pop3), los cuales son escaneados por las herramientas de nmap y nessus para conocer su estado de vulnerabilidad.

Diagnostico
La herramiente Nmap identifica los puertos asociados a los servicios de correo, el sistema operativo y el dominio cobranzasbeta.com.co, con el scaner del sistema Nesus se encuentran vulnerabilidades que deben ser evaluadas para identificar el nivel de exposicion a ataques externos y el risgo que se puede presentar con la no resolucion de las vulnerabilidades detetadas.

Herramientas Usadas	
Nombre herramienta	Descripcion
NMAP	La herramienta nmap identifica los puertos, el dominio, y el sistema operativo del servidor que esta asociado a la direcion Ip externa.
NESSUS	La herramienta nessus identifica 9 vulnerabilidades medias, 7 vulnerabilidades bajas y 29 items de informacion relevante en el escaneo

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

23

[23] Fuente Propia IP: 180.133.42.180

Formato de levantamiento Pentesting			
Fecha:			
Nombre:	Alexander Diaz P	# de ID	
Fase de Busquec			
IP:	MASk		

Puertos	Servicios Asociados	URL	A-Externo
80	HTTP (TCP)		ON

Comentarios
El servicio asociado a la direccion [redacted] pertenece al sitio web corporativo, el cual responde al dominio www.cobranzasbeta.com.co, en este servicio con la ayuda de la herramienta nmap se evidencia el sistema operativo, dominio y servicio de la pagina web, con la herramienta nessus se evidencian vulnerabilidades.

Diagnostico
la herramienta nessus luego de su scaner gerera 4 vulnerabilidades medias, una baja y 20 items de informacion. Lo que implica que se deben revisr para poder cerrar la brecha de riesgo a posibles ataques.

Herramientas Usadas	
Nombre herramienta	Descripcion
NMAP	Encuentra luego del scaner el puerto y el servicio asociado al dominio www.cobranzasbeta.com.co
NESSUS	Encuentra vulnerabilidades medias y bajas para poder ser mitigadas y cerrar la brecha de ataque.

Firmas de Aceptacion	
Alexander Diaz Pulido	Marcela Ramirez

24

[24] Fuente Propia IP: 180.34.136.234

ANEXO B

Informe de Escaneos con Nmap

Nmap Scan Report - Scanned at Sun Apr 30 11:59:17 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 11:59:17 2017 with these arguments:
nmap -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:10:09 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:10:09 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

25

[25] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:11:08 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:11:08 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:11:50 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:11:50 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

26

[26] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:00:09 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:00:09 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Hostnames

- mail.cobranzasbeta.com.co (PTR)

Ports

The 65526 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra ir
25	tcp	open	smtp	syn-ack	Postfix smtpd		
80	tcp	open	http	syn-ack			
110	tcp	open	pop3	syn-ack	Zimbra pop3d		
143	tcp	open	imap	syn-ack	Zimbra imapd		
443	tcp	open	http	syn-ack	Zimbra http config		
465	tcp	open	smtp	syn-ack	Postfix smtpd		
587	tcp	open	smtp	syn-ack	Postfix smtpd		
993	tcp	open	imap	syn-ack	Zimbra imapd		
995	tcp	open	pop3	syn-ack	Zimbra pop3d		

Remote Operating System Detection

- Used port: **25/tcp (open)**
- OS match: **Linux 2.6.32 or 3.10 (90%)**
- OS match: **Linux 2.6.32 (90%)**
- OS match: **Linux 2.6.39 (90%)**
- OS match: **Linux 3.1 - 3.2 (89%)**
- OS match: **Linux 3.8 (89%)**
- OS match: **Synology DiskStation Manager 5.1 (88%)**
- OS match: **Linux 3.4 (87%)**
- OS match: **WatchGuard Fireware 11.8 (87%)**
- OS match: **Linux 2.6.32 - 2.6.39 (86%)**
- OS match: **Linux 3.10 (86%)**

Traceroute Information

- Traceroute data generated using port 443/tcp

Hop	Rtt	IP	Host
1	2.00	192.168.100.1	dtv.test
3	100.00	10.100.10.1	
5	81.00	10.100.10.10	
7	81.00	206.223.124.139	telmex-nap.ccit.org.co
8	81.00	181.49.179.138	
9	63.00	10.175.23.254	
10	63.00	190.144.32.186	

Misc Metrics

Metric	Value
Ping Results	
System Uptime	439723 seconds (last reboot: Tue Apr 25 09:54:54 2017)
TCP Sequence Prediction	Difficulty=257 (Good luck!)
IP ID Sequence Generation	All zeros

27

[27] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 10:53:00 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 10:53:00 2017 with these arguments:
nmap -T4 -A -v

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Ports

The 996 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra
443	tcp	open	https	syn-ack			
1723	tcp	open	pptp	syn-ack	DrayTek	(Firmware: 1)	
8081	tcp	open	tcpwrapped	syn-ack			
8443	tcp	open	https-alt	syn-ack			

Remote Operating System Detection

- Used port: **443/tcp (open)**
- OS match: **Linksys BEFSR41 EtherFast router (87%)**
- OS match: **OneAccess 1641 router (86%)**
- OS match: **AVtech Room Alert 26W environmental monitor (85%)**

Traceroute Information

- Traceroute data generated using port 443/tcp

Hop	Rtt	IP	Host
2	23.00	172.31.252.242	
3	27.00	190.157.5.145	
4	25.00	206.223.124.193	
6	21.00	10.5.3.166	
7	26.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	
TCP Sequence Prediction	Difficulty=263 (Good luck!)
IP ID Sequence Generation	Incremental

28

[28] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:28:17 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:28:17 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:29:13 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:29:13 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

29

[29] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:29:47 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:29:47 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:30:34 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:30:34 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

30

[30] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:18:44 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:18:44 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:20:07 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:20:07 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:25:49 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:25:49 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

31

[31] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:26:43 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:26:43 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun Apr 30 12:27:28 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:27:28 2017 with these arguments:
nmap -p 1-65535 -T4 -A -v

Verbosity: 1; Debug level 0

(offline)

Address

- [redacted] - (ipv4)

Ports

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics

Metric	Value
Ping Results	

32

[32] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:57:30 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:57:30 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Ports

The 998 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra ir
8008	tcp	open	http	syn-ack	Apache httpd	2.2.15	
8443	tcp	open	http	syn-ack	Apache httpd	2.2.15	(CentOS

Remote Operating System Detection

- Used port: **8008/tcp (open)**
- OS match: **Linux 3.8 (91%)**
- OS match: **Linux 2.6.32 (90%)**
- OS match: **Linux 2.6.32 or 3.10 (90%)**
- OS match: **Linux 2.6.39 (90%)**
- OS match: **WatchGuard Fireware 11.8 (89%)**
- OS match: **Linux 3.1 - 3.2 (89%)**
- OS match: **Synology DiskStation Manager 5.1 (88%)**
- OS match: **Linux 3.10 (87%)**
- OS match: **Linux 3.4 (87%)**
- OS match: **Linux 2.6.32 - 2.6.39 (86%)**

Traceroute Information

- Traceroute data generated using port 8443/tcp

Hop	Rtt	IP	Host
1	1.00	192.168.100.1	dtv.test
3	25.00	10.100.10.1	
5	28.00	10.100.10.10	
7	39.00	206.223.124.139	telmex-nap.ccit.org.co
8	30.00	181.49.179.138	
9	31.00	10.175.23.254	
10	31.00	190.144.32.186	

Misc Metrics

Metric	Value
Ping Results	
System Uptime	406422 seconds (last reboot: Tue Apr 25 20:05:11 2017)
TCP Sequence Prediction	Difficulty=257 (Good luck!)
IP ID Sequence Generation	All zeros

33

[33] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 13:02:32 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 13:02:32 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	2.00	192.168.100.1	dtv.test
3	59.00	10.100.10.1	
5	60.00	10.100.10.10	
6	60.00	190.131.192.61	
7	60.00	206.223.124.139	telmex-nap.ccit.org.co
8	60.00	181.49.179.138	
9	61.00	10.175.23.254	

Misc Metrics

Metric	Value
Ping Results	

34

[34] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 13:06:48 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 13:06:48 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	2.00	192.168.100.1	dtv.test
3	40.00	10.100.10.1	
5	40.00	10.100.10.10	
6	41.00	190.131.192.61	
7	47.00	206.223.124.139	telmex-nap.ccit.org.co
8	47.00	181.49.179.138	
9	41.00	10.175.23.254	

Misc Metrics

Metric	Value
Ping Results	

35

[35] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 13:10:35 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 13:10:35 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	1.00	192.168.100.1	dtv.test
3	50.00	10.100.10.1	
5	51.00	10.100.10.10	
6	51.00	190.131.192.61	
7	65.00	206.223.124.139	telmex-nap.ccit.org.co
8	52.00	181.49.179.138	
9	44.00	10.175.23.254	

Misc Metrics

Metric	Value
Ping Results	

36

[36] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 13:14:20 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 13:14:20 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Hostnames

- [redacted]

Ports

The 991 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra i
25	tcp	open	smtp	syn-ack	Postfix smtpd		
80	tcp	open	http	syn-ack			
110	tcp	open	pop3	syn-ack	Zimbra pop3d		
143	tcp	open	imap	syn-ack	Zimbra imapd		
443	tcp	open	http	syn-ack	Zimbra http config		
465	tcp	open	smtp	syn-ack	Postfix smtpd		
587	tcp	open	smtp	syn-ack	Postfix smtpd		
993	tcp	open	imap	syn-ack	Zimbra imapd		
995	tcp	open	pop3	syn-ack	Zimbra pop3d		

Remote Operating System Detection

- Used port: **25/tcp (open)**
- OS match: **Linux 3.8 (91%)**
- OS match: **Linux 2.6.32 (90%)**
- OS match: **Linux 2.6.39 (90%)**
- OS match: **Linux 3.10 (89%)**
- OS match: **Linux 3.4 (89%)**
- OS match: **WatchGuard Fireware 11.8 (89%)**
- OS match: **Linux 3.1 - 3.2 (89%)**
- OS match: **Linux 2.6.32 or 3.10 (89%)**
- OS match: **Synology DiskStation Manager 5.1 (88%)**
- OS match: **Linux 2.6.32 - 2.6.39 (86%)**

Traceroute Information

- Traceroute data generated using port 587/tcp

Hop	Rtt	IP	Host
1	2.00	192.168.100.1	dtv.test
3	30.00	10.100.10.1	
5	110.00	10.100.10.10	
7	34.00	206.223.124.139	telmex-nap.ccit.org.co
8	35.00	181.49.179.138	
9	21.00	10.175.23.254	
10	22.00	190.144.32.186	

Misc Metrics

Metric	Value
Ping Results	
System Uptime	484399 seconds (last reboot: Mon Apr 24 22:42:31 2017)
TCP Sequence Prediction	Difficulty=262 (Good luck!)
IP ID Sequence Generation	All zeros

37

[37] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun May 28 21:36:16 2017

Scan Summary

Nmap 7.31 was initiated at Sun May 28 21:36:16 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Hostnames

- [redacted] (PTR)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	15.00	186.81.164.1	static-ip-186811641.cable.net.co
2	21.00	172.31.252.242	
3	24.00	190.157.5.145	static-ip-1901575145.cable.net.co
4	26.00	206.223.124.193	etb1-nap.ccit.org.co
7	25.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

38

[38] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun May 28 20:29:53 2017

Scan Summary

Nmap 7.31 was initiated at Sun May 28 20:29:53 2017 with these arguments:
nmap -T4 -A -v -Pn nmap

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Hostnames

- (PTR)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	18.00	186.81.164.1	static-ip-186811641.cable.net.co
2	22.00	172.31.252.246	
3	23.00	190.157.5.145	static-ip-1901575145.cable.net.co
4	37.00	206.223.124.193	etb1-nap.ccit.org.co
6	15.00	10.5.2.166	
7	41.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun May 28 21:51:34 2017

Scan Summary

Nmap 7.31 was initiated at Sun May 28 21:51:34 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	19.00	186.81.164.1	
2	23.00	172.31.253.14	
3	34.00	190.157.5.145	
6	27.00	10.5.2.166	

Misc Metrics

Metric	Value
Ping Results	

Nmap Scan Report - Scanned at Sun May 28 21:53:33 2017

Scan Summary

Nmap 7.31 was initiated at Sun May 28 21:53:33 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Hostnames

-

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	16.00	186.81.164.1	static-ip-186811641.cable.net.co
2	23.00	172.31.253.110	
3	26.00	190.157.5.145	static-ip-1901575145.cable.net.co
4	18.00	206.223.124.193	etb1-nap.ccit.org.co
6	38.00	10.5.2.166	
7	18.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

39

[39] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 10:45:52 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 10:45:52 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Hostnames

- [redacted]

Ports

The 996 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra
443	tcp	open	https	syn-ack			
1723	tcp	open	pptp	syn-ack	DrayTek	(Firmware: 1)	
8081	tcp	open	tcpwrapped	syn-ack			
8443	tcp	open	https-alt	syn-ack			

Remote Operating System Detection

- Used port: **443/tcp (open)**
- OS match: **Linksys BEFSR41 EtherFast router (87%)**
- OS match: **OneAccess 1641 router (86%)**
- OS match: **AVtech Room Alert 26W environmental monitor (85%)**

Traceroute Information

- Traceroute data generated using port 443/tcp

Hop	Rtt	IP	Host
2	23.00	172.31.252.242	
3	25.00	190.157.5.145	static-ip-1901575145.cable.net.co
4	27.00	206.223.124.193	etb1-nap.ccit.org.co
6	26.00	10.5.2.166	
7	21.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	
TCP Sequence Prediction	Difficulty=263 (Good luck!)
IP ID Sequence Generation	Incremental

40

[40] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Sun Apr 30 12:38:49 2017

Scan Summary

Nmap 7.40 was initiated at Sun Apr 30 12:38:49 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Hostnames

-

Ports

The 998 ports scanned but not shown below are in state: **filtered**

Port	State	Service	Reason	Product	Version	Extra i
80 tcp	open	http	syn-ack	Apache httpd	2.4.18	(Ubuntu

Remote Operating System Detection

- Used port: **80/tcp (open)**
- Used port: **25/tcp (closed)**
- OS match: **Linux 3.11 - 4.1 (93%)**
- OS match: **Linux 3.8 (93%)**
- OS match: **Linux 3.16 (91%)**
- OS match: **Linux 3.13 (89%)**
- OS match: **Linux 2.6.32 (88%)**
- OS match: **Linux 4.0 (88%)**
- OS match: **Linux 3.0 (87%)**
- OS match: **Linux 4.4 (87%)**
- OS match: **Linux 3.2 - 3.8 (87%)**
- OS match: **Linux 3.10 - 3.12 (86%)**

Traceroute Information

- Traceroute data generated using port 25/tcp

Hop	Rtt	IP	Host
1	1.00	192.168.100.1	dtv.test
3	71.00	10.100.10.1	
5	70.00	10.100.10.10	
7	71.00	206.223.124.193	etb1-nap.ccit.org.co

Misc Metrics

Metric	Value
Ping Results	
System Uptime	9394286 seconds (last reboot: Wed Jan 11 19:08:18 2017)
TCP Sequence Prediction	Difficulty=261 (Good luck!)
IP ID Sequence Generation	All zeros

41

[41] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 11:25:57 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 11:25:57 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

Address

- [redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	71.00	186.81.164.1	
2	23.00	172.31.252.242	
3	43.00	190.157.5.145	
4	54.00	206.223.124.193	
6	17.00	10.5.2.166	
7	20.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

42

[42] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 14:25:43 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 14:25:43 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

online)

Address

- - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	23.00	186.81.164.1	
2	20.00	172.31.252.246	
3	24.00	190.157.5.145	
4	38.00	206.223.124.193	
6	16.00	10.5.3.166	
7	40.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

43

[43] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 15:15:20 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 15:15:20 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- [redacted] - (ipv4)

Hostnames

- [redacted]

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information

- Traceroute data generated using port /icmp

Hop	Rtt	IP	Host
1	16.00	186.81.164.1	static-ip-186811641.cable.net.co
2	22.00	172.31.253.14	
4	25.00	206.223.124.193	etb1-nap.ccit.org.co
6	46.00	10.5.3.166	
7	25.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	

44

[44] Reportes Escaneo NMAP

Nmap Scan Report - Scanned at Mon May 29 16:53:12 2017

Scan Summary

Nmap 7.31 was initiated at Mon May 29 16:53:12 2017 with these arguments:
nmap -T4 -A -v -Pn

Verbosity: 1; Debug level 0

(online)

Address

- - (ipv4)

Hostnames

-

Ports

The 999 ports scanned but not shown below are in state: **filtered**

Port		State	Service	Reason	Product	Version	Extra
8500	tcp	open	http	syn-ack	mini_httpd	1.19 19dec2003	

Remote Operating System Detection

- Used port: **8500/tcp (open)**
- OS match: **Linux 3.2 - 3.8 (100%)**

Traceroute Information

- Traceroute data generated using port 8500/tcp

Hop	Rtt	IP	Host
2	44.00	172.31.253.110	
3	43.00	190.157.5.145	static-ip-1901575145.cable.net.co
4	37.00	206.223.124.193	etb1-nap.ccit.org.co
6	38.00	10.5.2.166	
7	31.00	10.248.237.2	

Misc Metrics

Metric	Value
Ping Results	
System Uptime	1743877 seconds (last reboot: Tue May 09 12:30:34 2017)
TCP Sequence Prediction	Difficulty=258 (Good luck!)
IP ID Sequence Generation	All zeros

45

[45] Reportes Escaneo NMAP

ANEXO C

Informes de Escaneos de Nessus

Tenable.io Report

Tenable.io Report

Tue, 30 May 2017 15:40:56 UTC

Table Of Contents

46

[46] Reportes Escaneo Nessus

40984 (1) - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

www. .com.co (tcp/80) Vulnerability State: Active

```
The following directories are browsable  :

http://www.cobranzas .com.co/chat/images/
http://www.cobranzas .com.co/chat/images/buttons/
http://www.cobranza s .com.co/chat/images/geo/
http://www.cobranzas t.com.co/chat/images/geo/default/
http://www.cobranzas .com.co/c hat/images/payment/
http://www.cobranzas .com.co/chat/images/smilies/
```

47

[47] Reportes Escaneo Nessus

94437 (10) - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.
Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

See Also

https://sweet32.info

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.8 (E:F/RL:ND/RC:ND)

References

CVE	CVE-2016-6329
CVE	CVE-2016-2183
BID	92631
BID	92630
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/8443) Vulnerability State: Active

```
List of 64-bit block cipher suites supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
```

48

[48] Reportes Escaneo Nessus

```
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

[redacted] (tcp/587) Vulnerability State: Active

```
List of 64-bit block cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    TLSv1
      EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ADH-DES-CBC3-SHA            Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA      Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      AECDH-DES-CBC3-SHA          Kx=ECDH        Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

11229 (1) - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :
- The username of the user who installed PHP and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

www [redacted] com.co (tcp/80) Vulnerability State: Active

```
Nessus discovered the following URL that calls phpinfo() :

  - http://www.cobranzas[redacted].com.co/info.php
```

49

[49] Reportes Escaneo Nessus

55640 (1) - SQL Dump Files Disclosed via Web Server

Synopsis

The remote web server hosts publicly accessible SQL dump files.

Description

The remote web server hosts publicly available files that contain SQL instructions. These files are most likely database dumps and may contain sensitive information.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

www [redacted].com.co (tcp/80) Vulnerability State: Active

```
The following SQL files are available on the remote server :

  - /chat/images/cobranza_chat.sql
```

50

[50] Reportes Escaneo Nessus

20007 (1) - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of 'strong cryptography'.

See Also

http://www.schneier.com/paper-ssl.pdf

http://support.microsoft.com/kb/187498

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/465) Vulnerability State: Active

```
- SSLv3 is enabled and the server supports at least one cipher.
```

51

[51] Reportes Escaneo Nessus

57582 (3) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/443) Vulnerability State: Active

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=TW/ST=HsinChu/L=HuKou/O=DrayTek Corp./OU=DrayTek Support/CN=Vigor Router
```

[redacted] (tcp/25) Vulnerability State: Active

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=co/ST=Cundinamarca/L=Bogota/O=Cobranzas Beta/OU=Sistemas/CN=mx.cobranzasbeta.com.co/
E=admin@cobranzasbeta.com.co
```

52

[52] Reportes Escaneo Nessus

51192 (10) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/443) Vulnerability State: Active

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=TW/ST=HsinChu/L=HuKou/O=DrayTek Corp./OU=DrayTek Support/CN=Vigor Router
|-Issuer  : C=TW/ST=HsinChu/L=HuKou/O=DrayTek Corp./OU=DrayTek Support/CN=Vigor Router
```

[redacted] (tcp/25) Vulnerability State: Active

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=co/ST=Cundinamarca/L=Bogota/O=Cobranzas [redacted]/OU=Sistemas/CN=mx.cobranzas[redacted].com.co/
E=admin@cobranza[redacted].com.co
|-Issuer  : C=co/ST=Cundinamarca/L=Bogota/O=Cobranzas [redacted]/OU=Sistemas/CN=mx.cobranzas[redacted].com.co/
E=admin@cobranza[redacted].com.co
```

53

[53] Reportes Escaneo Nessus

42873 (10) - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/8443) Vulnerability State: Active

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  The fields above are :

    {OpenSSL ciphername}
    Kx={key exchange}
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

[redacted] (tcp/465) Vulnerability State: Active

```
  Here is the list of medium strength SSL ciphers supported by the remote server :

    Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

      TLSv1
        EDH-RSA-DES-CBC3-SHA          Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
        ADH-DES-CBC3-SHA              Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
        ECDHE-RSA-DES-CBC3-SHA        Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
        AECDH-DES-CBC3-SHA            Kx=ECDH        Au=None     Enc=3DES-CBC(168)        Mac=SHA1
        DES-CBC3-SHA                  Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  The fields above are :

    {OpenSSL ciphername}
    Kx={key exchange}
    Au={authentication}
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

54

[54] Reportes Escaneo Nessus

85582 (1) - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

http://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:693

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

www.[redacted].com.co (tcp/80) Vulnerability State: Active

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/config.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/copyright.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/credits.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/developers.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/genindex.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/glossary.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/import_export.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/index.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/intro.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/other.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/privileges.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/require.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/search.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/setup.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/transformations.html
  - http://www.cobranzas    .com.co/phpmyadmin/doc/html/user.html
```

55

[55] Reportes Escaneo Nessus

45411 (1) - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The commonName (CN) of the SSL certificate presented on this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] **(tcp/25) Vulnerability State: Active**

```
The identities known by Nessus are :

  pop.cobranzas     .com.co
  smtp.cobranzas     .com.co
  mail.cobranzas     .com.co

The Common Name in the certificate is :

  mx.cobranzas     com.co
```

56

[56] Reportes Escaneo Nessus

81606 (1) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

https://www.smacktls.com/#freak

https://www.openssl.org/news/secadv/20150108.txt

http://www.nessus.org/u?b78da2c4

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

4.1 (E:F/RL:OF/RC:ND)

References

CVE	CVE-2015-0204
BID	71936
XREF	CERT:243585
XREF	OSVDB:116794

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/587) Vulnerability State: Active

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    TLSv1
      EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
      EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57

[57] Reportes Escaneo Nessus

35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

http://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

3.5 (E:ND/RL:OF/RC:C)

References

CVE	CVE-2004-2761
BID	11849
BID	33065
XREF	OSVDB:45127
XREF	OSVDB:45108
XREF	OSVDB:45106
XREF	CWE:310
XREF	CERT:836068

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/25) Vulnerability State: Active

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : C=co/ST=Cundinamarca/L=Bogota/O=Cobranzas [redacted] /OU=Sistemas/
CN=mx.cobranzas[redacted].com.co/E=admin@cobranzas[redacted].com.co
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 08 12:46:06 2016 GMT
|-Valid To            : Jul 06 12:46:06 2026 GMT
```

58

[58] Reportes Escaneo Nessus

26928 (2) - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:928
XREF	CWE:803
XREF	CWE:934

[59]

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/25) Vulnerability State: Active

```
Here is the list of weak SSL ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    TLSv1
      EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1
      DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

[59] Reportes Escaneo Nessus

91572 (2) - OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Synopsis

It was possible to obtain sensitive information from the remote host with TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256.
The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.

See Also

https://blog.filippo.io/luckyminus20/

http://www.nessus.org/u?37b909b6

https://www.openssl.org/news/secadv/20160503.txt

Solution

Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2107
BID	89760
XREF	OSVDB:137896
XREF	EDB-ID:39768

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] **(tcp/465) Vulnerability State: Active**

```
Nessus was able to trigger a RECORD_OVERFLOW alert in the
remote service by sending a crafted SSL "Finished" message.
```

60

[60] Reportes Escaneo Nessus

31705 (3) - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.3 (E:ND/RL:OF/RC:C)

References

CVE	CVE-2007-1858
BID	28482
XREF	OSVDB:34882

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/587) Vulnerability State: Active

```
Here is the list of SSL anonymous ciphers supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    TLSv1
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
export
      ADH-DES-CBC-SHA              Kx=DH          Au=None     Enc=DES-CBC(56)          Mac=SHA1

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      ADH-DES-CBC3-SHA             Kx=DH          Au=None     Enc=3DES-CBC(168)        Mac=SHA1
      AECDH-DES-CBC3-SHA           Kx=ECDH        Au=None     Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      ADH-AES128-SHA               Kx=DH          Au=None     Enc=AES-CBC(128)         Mac=SHA1
      ADH-AES256-SHA               Kx=DH          Au=None     Enc=AES-CBC(256)         Mac=SHA1
      ADH-CAMELLIA128-SHA          Kx=DH          Au=None     Enc=Camellia-CBC(128)    Mac=SHA1
      ADH-CAMELLIA256-SHA          Kx=DH          Au=None     Enc=Camellia-CBC(256)    Mac=SHA1
      ADH-RC4-MD5                  Kx=DH          Au=None     Enc=RC4(128)             Mac=MD5
      ADH-SEED-SHA                 Kx=DH          Au=None     Enc=SEED-CBC(128)        Mac=SHA1
      AECDH-AES128-SHA             Kx=ECDH        Au=None     Enc=AES-CBC(128)         Mac=SHA1
      AECDH-AES256-SHA             Kx=ECDH        Au=None     Enc=AES-CBC(256)         Mac=SHA1
      AECDH-RC4-SHA                Kx=ECDH        Au=None     Enc=RC4(128)             Mac=SHA1
```

61

[61] Reportes Escaneo Nessus

54582 (1) - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

http://tools.ietf.org/html/rfc4422

http://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/25) Vulnerability State: Active

```
The SMTP server advertises the following SASL methods over an
unencrypted channel :

  All supported methods : PLAIN, LOGIN, DIGEST-MD5, CRAM-MD5
  Cleartext methods     : PLAIN, LOGIN
```

15855 (1) - POP3 Cleartext Logins Permitted

Synopsis

The remote POP3 daemon allows credentials to be transmitted in cleartext.

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

See Also

http://tools.ietf.org/html/rfc2222

http://tools.ietf.org/html/rfc2595

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/110) Vulnerability State: Active

```
The following cleartext methods are supported :
USER
SASL PLAIN X-ZIMBRA
EXPIRE 31 USER
```

62

[62] Reportes Escaneo Nessus

12224 (3) - Web Server Load Balancer Detection

Synopsis

The remote web server is load-balanced.

Description

The remote web server seems to be running in conjunction with several others behind a load balancer. Knowing that there are multiple systems behind a service could be useful to an attacker as the underlying hosts may be running different operating systems, patchlevels, etc.

Solution

Update the web configuration to hide information disclosure.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/8443) Vulnerability State: Active

```
Nessus queried the remote web server 20 times and was redirected to
the following locations :

  https://static-            .8.static.etb.net.co/images/
  https://static-            .8.static.etb.net.co:8081/images/
  https://static-            .8.static.etb.net.co:8443/images/
  https://static-            .8.static.etb.net.co:8081/images/
  https://static-            .8.static.etb.net.co:8443/images/
  https://static-            .8.static.etb.net.co/images/
  https://static-            .8.static.etb.net.co:8081/images/
  https://static-            .8.static.etb.net.co:8443/images/
  https://static-            .8.static.etb.net.co/images/
  https://static-            .8.static.etb.net.co:8081/images/
```

63

[63] Reportes Escaneo Nessus

65821 (8) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

2.2 (E:F/RL:TF/RC:ND)

References

CVE	CVE-2013-2566
CVE	CVE-2015-2808
BID	73684
BID	58796
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] **(tcp/25) Vulnerability State: Active**

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      ADH-RC4-MD5                 Kx=DH          Au=None      Enc=RC4(128)             Mac=MD5
      RC4-MD5                     Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
```

64

[64] Reportes Escaneo Nessus

83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

http://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)

References

CVE	CVE-2015-4000
BID	74733
XREF	OSVDB:122331

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

65

Assets

[redacted] (tcp/587) Vulnerability State: Active

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)
```

[65] Reportes Escaneo Nessus

83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

2.2 (E:F/RL:TF/RC:ND)

References

CVE	CVE-2015-4000
BID	74733
XREF	OSVDB:122331

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

Assets

[redacted] (tcp/587) Vulnerability State: Active

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-ADH-DES-CBC-SHA          Kx=DH(512)     Au=None     Enc=DES-CBC(40)          Mac=SHA1
 export
      EXP-ADH-RC4-MD5              Kx=DH(512)     Au=None     Enc=RC4(40)              Mac=MD5
 export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

66

[66] Reportes Escaneo Nessus

26194 (1) - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:930
XREF	CWE:928
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 0000/00/00, Modification date: 0000/00/00

67

Assets

www. [redacted] com.co (tcp/80) Vulnerability State: Active

```
Page : /phpmyadmin/
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/index.php
Destination Page: /phpmyadmin/index.php
```

[67] Reportes Escaneo Nessus

ANEXO D

Informe Final

EVALUAR EL ESTADO DE LA SEGURIDAD DE ACCESO POR MEDIO DE UN TEST DE INTRUSIÓN DE LA EMPRESA ASESORÍAS EN COBRANZAS MEGACOBRO, PARA LA IDENTIFICACIÓN DE SUS VULNERABILIDADES Y SUS REMEDIACIONES

Especialización Seguridad Informática

Ingenieros:

Ing. Alexander Díaz Pulido
Ing. Marcela Ramírez

27/06/2017
Bogota, Colombia

Glosario

CONTROLES (ISO 27001): las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

HARDERING: Es el proceso de asegurar y reforzar los controles y Seguridad de los Sistemas para mitigar las vulnerabilidades o brechas de Seguridad de la que pueden aprovecharse los atacantes.

IP "*INTERNET PROTOCOL*": es el número de identificación de un dispositivo en una red.

IP PÚBLICA: es el número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red, este número identifica el punto de enlace con Internet.

PENTESTING: Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

RIESGOS (ISO 27001): Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO RESIDUAL (ISO 27001): El riesgo que permanece tras el tratamiento del riesgo.

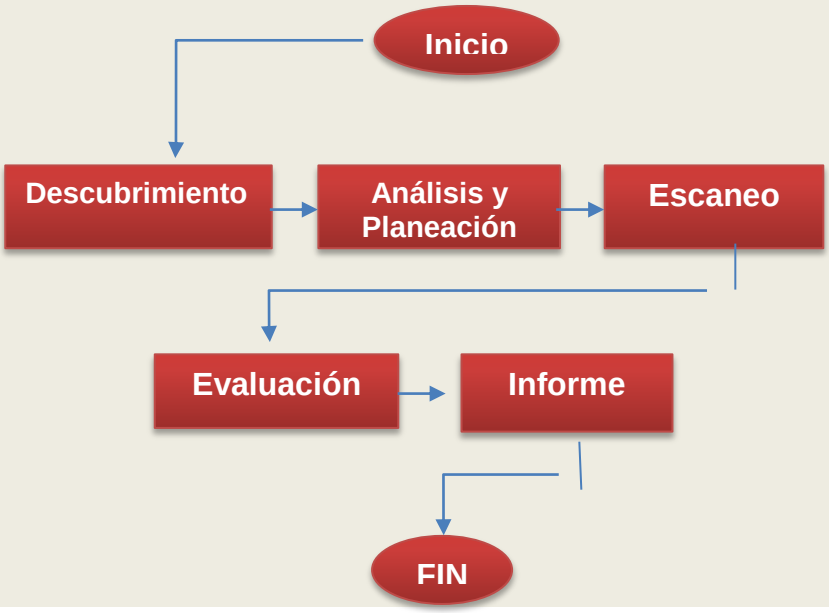
SEGURIDAD DE LA INFORMACIÓN (ISO 27001): preservación de la confidencialidad, integridad y disponibilidad de la información.

SOFTWARE: es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

VULNERABILIDAD (ISO 27001): debilidad de un activo o control que puede ser explotada por una o más amenazas.

Resumen ejecutivo

Actualmente las empresas presentan una gran cantidad de ataques informáticos a través de Internet, por ese motivo se deben de tomar las medidas necesarias para identificar las vulnerabilidades y mitigar los riesgos a los que se pueden estar expuestos. Es por esto por lo que se planteó la necesidad de generar un diagnóstico de seguridad realizando un Pentesting a las IP´s públicas de la compañía, realizando diferentes actividades de escaneo, revisión y análisis, para poder identificar las vulnerabilidades y brechas de seguridad que pueden ser aprovechadas por los atacantes informáticos. Dentro del proceso del Pentesting realizado durante un periodo de actividades se pudo concluir este proceso con 64 hallazgos de vulnerabilidades en las aplicaciones asociadas a las IP,s públicas, las cuales están catalogadas como medias y bajas según la herramienta de escaneo de vulnerabilidades Nessus, y luego de un análisis de los hallazgos por parte de los ingenieros que realizaron las actividades de ejecución del Pentesting; estos hallazgos representan el nivel de exposición frente a los ataques externos por lo tanto deben ser atendidos de la mejor manera y seguir las recomendaciones de mitigación que son expuestas para cerrar la brecha de seguridad y asegurar en mayor medida la información de la compañía a los ataques informáticos desde Internet.



[68]

[68] Metodología Pentesting

Para la simulación de ataques externos se tienen en cuenta, el enfoque de sombrero negro y sombrero gris, es decir, en el enfoque de sombrero negro no se tiene ningún tipo de información y para las actividades de descubrimiento de datos del objetivo se toman en cuenta los medios públicos existentes en Internet, simulando al 100% como un atacante encuentra datos para atacar, es medir el nivel de exposición de la compañía con datos y fuentes de acceso público; en el enfoque de sombrero gris se entregan datos para el Pentesting y se complementa con lo encontrado en el otro enfoque para estructurar mejor las actividades posteriores de escaneo.

Como resultado de las actividades del Pentesting se pudo hallar una serie de vulnerabilidades expuestas y repetitivas en los servicios y servidores asociados a las IP´s públicas y las cuales luego de un análisis se pudieron clasificar en 3 grupos de acuerdo con la naturaleza de exposición o criticidad y a la importancia dada por su hallazgo:

- Protocolos de cifrado y certificados de Seguridad
- Fallas de Configuración.
- Fallas de Hardering.

El primer grupo, hace referencia a los hallazgos en los cuales el manejo de protocolos de cifrado usados en las comunicaciones de los servicios y/o servidores es obsoleta, ya que usan algoritmos de cifrado muy débil como el uso de algoritmos criptográficos DES, Diffie-Hellman o SHA1 en el cálculo de los códigos de HASH dentro de las configuraciones.

De igual manera en este grupo se evidencia el uso de certificados SSL auto-firmados, no reconocidos y obsoletos en sus versiones más antiguas las cuales son vulnerables.

El segundo grupo, hace referencia a fallas de Configuración, fallas no detectadas en el momento de su paso a producción, pero que pueden exponer los servicios y la información contenida en servidores expuestos a Internet, es el caso de los archivos infophp.php los cuales fueron identificados en el servidor de producción escaneado y el cual puede dar información valiosa de las configuraciones a los atacantes informáticos.

Por último, fueron encontrados hallazgos que hacen referencia a fallas de hardering, que evidencian pocos controles cuando un servicio o

servidor va a ser publicado por Internet, es el caso de los archivos SQL que fueron hallados y los cuales no deben estar expuestos ya que contienen información muy importante.

Luego de estos hallazgos se proponen actividades las cuales podrían minimizar el riesgo de exposición a los ataques informáticos al realizar las actividades propuestas de remediación.

Lista de Vulnerabilidades

- El servicio remoto admite el uso de cifrado de bloques de 64 bits.
- Algunos directorios en el servidor web remoto son navegables.
- El servidor web remoto contiene un script PHP que es propenso a un ataque de divulgación de información.
- El servidor web aloja archivos de SQL de acceso público.
- El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.
- Certificado SSL auto-firmado.
- El certificado SSl no es confiable.
- Cifrado SSL compatible y de mediana fuerza.
- La aplicación Web potencialmente vulnerable a Clickjacking.
- Certificado SSl con nombre de host incorrecto.
- SSL / TLS EXPORT_RSA <= Complementos de cifrado de 512 bits compatibles (FREAK).
- Certificado SSL firmado utilizando algoritmo de hash débil.
- Divulgación de información de tipo man-in-the-middle (MitM) debido a un error en la implementación de AES-NI de OpenSSl.
- El servicio remoto admite el uso de cifrados SSL anónimos.
- El servidor de correo permite login SMTP de sesión en texto plano.

- Login de sesión de POP3 en texto plano.
- El servicio remoto admite el uso del cifrado RC4.
- El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman inferiores o iguales a 1024 bits.
- SSL / TLS EXPORT_DHE <= 512 bits Exportación de cifrado Suites compatibles.
- El servidor web remoto puede transmitir las credenciales en texto sin cifrar.

Remediaciones:

En consideración de los hallazgos se concluyó que las remediaciones más adecuadas para mitigar los riesgos asociados a las vulnerabilidades encontradas son:

1. Adquisición de certificados de seguridad SSL/TLS a autoridades certificadoras por parte de la Empresa, para garantizar que se mitigue la vulnerabilidad asociada a las aplicaciones que tienen hallazgos al uso de certificados desconocidos, auto-firmados, obsoletos y/o no válidos.

   Se recomienda la adquisición, instalación y Configuración de estos certificados digitales a los servicios web asociados a las IP´s públicas, para autenticar y cifrar la información de una manera segura y confiable.

2. Realizar la revisión general de las configuraciones de los servicios y comunicaciones que realicen uso de cifrado débil y quitar de las configuraciones algoritmos criptográficos vulnerables como DES, 3DES, Diffie-Helman, algoritmos de hash como SHA y SHA1 e implementar métodos de cifrado más robusto.

3. Implementar un proceso de hardering exhaustivo para los servidores y servicios publicados, teniendo en cuenta los puertos necesarios para los servicios, el cifrado, los certificados de seguridad, los medios de autenticación e intentos simultáneos, las configuraciones de los servicios web para evitar ataques de DDoS, phishing, inyección de SQL, e implementar sistemas de

protección contra ataques de fuerza bruta, como Fail2ban o cualquier otro software de vaneo de IP por intentos de autenticación no válidos.

4. Implementar un proceso de Pentesting o búsqueda de vulnerabilidades periódico para descubrir posibles riesgos que deban ser mitigados y así generar mayor seguridad a la información y activos de la compañía.

Objetivos

Para realizar las actividades necesarias de diagnosticar la seguridad de las IP's públicas de la empresa se planteó el cumplimiento de los siguientes objetivos:

Objetivo General

Diagnosticar la Seguridad Informática por medio de un Pentesting a las IP's públicas de la empresa, en busca de posibles vulnerabilidades con el fin de sugerir remediaciones basado en los resultados obtenidos.

Objetivos específicos

- Realizar un cronograma de Pentesting para la ejecución de ataques controlados a las IP´s públicas de la compañía.
- Seleccionar una metodología para el test de intrusión.
- Ejecutar un plan de pruebas de intrusión de acuerdo con la metodología seleccionada.
- Analizar los hallazgos encontrados con el test de intrusión.
- Presentar un informe de remediación y/o conclusiones frente a los datos arrojados en la evaluación.

Impactos para la Compañía

Los datos de la compañía son el activo más valioso, dado que en ellos se encuentra el insumo para realizar las operaciones diarias y los procesos que se requieren para desarrollar la actividad económica, además no hay que olvidar que los datos personales de los clientes hay que resguardarlos en mayor medida y es por esto que la seguridad informática es tan importante y debe velar por mitigar los riesgos y las vulnerabilidades identificadas, ya que al no tener una buena práctica de asegurar la información y mitigar los riesgos producto de las vulnerabilidades que se tengan la compañía se expone a perdidas tanto económicas, perdida de reputación en el mercado y las sanciones legales que pueden ocasionarse por perdidas de información, producto de los ataques informáticos.

Sanciones Legales

Dentro de la legislación colombiana hay que tener en cuenta las posibles sanciones que se pueden obtener por divulgación de datos personales, los cuales pueden ser sancionados por la Superintendencia de Industria y Comercio en un eventual suceso de perdida de información y divulgación de bases de clientes. Por ejemplo, por una violación a la Ley 1581 la sanción pude llegar a los 2000 SMMLV (Salario Mínimo Mensuales Legales Vigentes), sumado a esto se puede también, tomar medidas de suspensión de actividades, cierre parcial o definitivo de la compañía.

Perdidas Reputaciones

La materialización de los riesgos por causa de eventos de seguridad informática exponen a la empresa, no solo a pérdidas económicas, o sanciones legales, sino también a perdidas reputaciones las cuales pueden ser más serias, ya que atenta con la competitividad en el mercado, la satisfacción de los clientes por los servicios ofrecidos, la fluidez y fidelización de los mismos, entre otros factores, los cuales pueden atentar aún más con el hecho de perder la información de la compañía por un evento de hacker o de delincuencia informática.

Pérdidas Económicas

Los ataques informáticos en el mundo dejan millones de dólares en pérdidas para las compañías cada año, información de clientes, vulneraciones a los sistema son cada día aumentan debido a las vulnerabilidades presentes y las cuales no son mitigadas y aprovechadas por los delincuentes; según el estudio realizado por Fortinet del panorama de la seguridad informática en Colombia, se encontró que más del 80 por ciento de las compañías en el país poseen sistemas altamente vulnerables, y estos pueden representar al país una gran cantidad de dinero en pérdidas económicas.

De igual manera, los costos asociados al cibercrimen de acuerdo con una encuesta sobre el Estado Global de Seguridad de la Información publicada por Price Water House Cooper, el impacto económico global se estimó en US$ 575.000 millones en 2015, donde América Latina y el Caribe sumaron costos por US$ 90.000 millones anuales, representando el 16% del costo total mundial del delito y cuatro veces más que la inversión social internacional. (Espectador 27 de octubre de 2016)

En el caso particular del riesgo económico está asociado a las posibles multas que un evento de robo de información de clientes puede ocasionar los cuales pueden estar asociados a sanciones de la Superintendencia de Industria y Comercio por mal manejo de datos personales de clientes, con esto, los daños reputaciones pueden desvirtuar la fidelidad de los clientes y puede afectar el mercado de la compañía.

Conclusiones Finales

El pentesting desarrollado para la búsqueda de vulnerabilidades a los servicios asociados a las IP´s públicas de la compañía sólo es un proceso inicial de diagnóstico de la seguridad informática que se puede realizar, ya que solo se ha escaneado una pequeña porción de los sistemas de comunicación e información orientados a lo expuesto en Internet; para poder tener una verdadera percepción de seguridad, se deben realizar procesos más elaborados y exhaustivos de todos los activos de la información, evaluando los riesgos y los controles

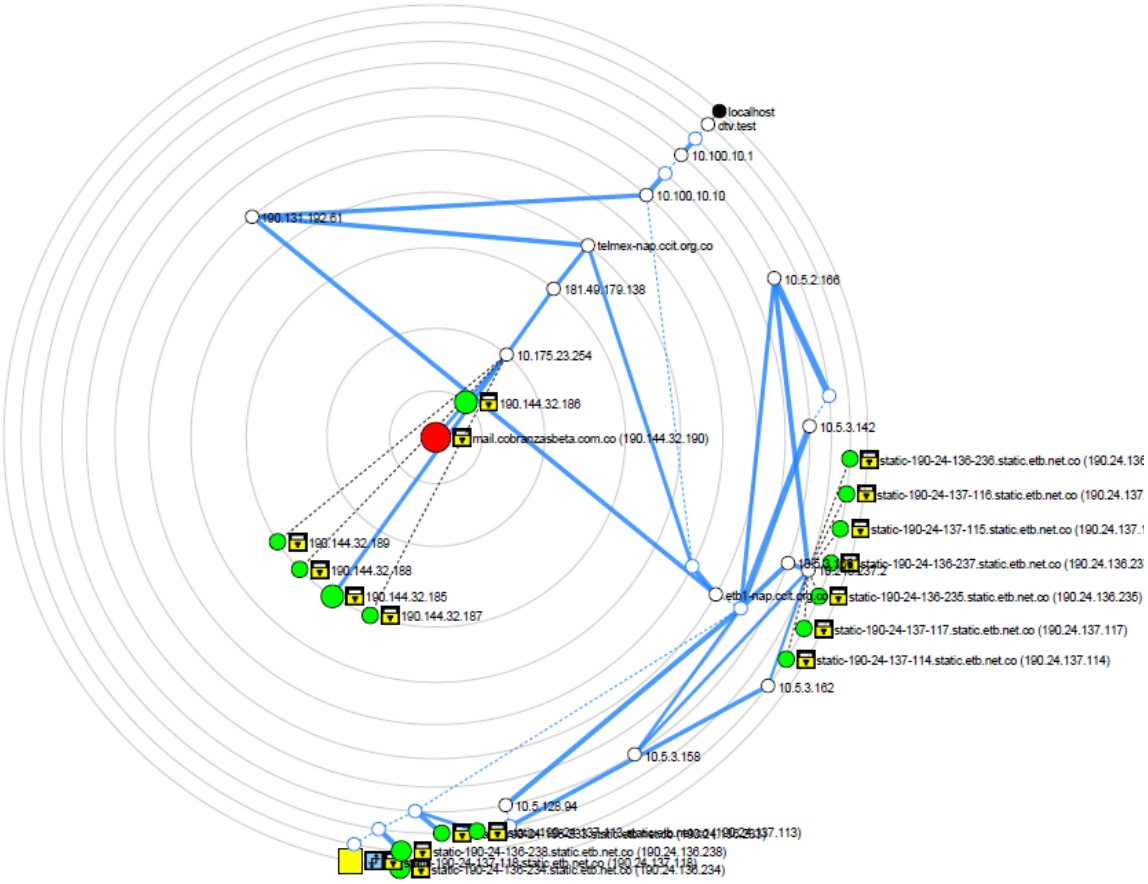
asociados para mitigarlos.

En este proceso de búsqueda y análisis de vulnerabilidades se logró constatar que existen vulnerabilidades que pueden afectar la información de la compañía, ocasionado por la exposición a Internet y a posibles ataques informáticos, por tal motivo, se deben tener en cuenta las remediaciones sugeridas para mitigar los riesgos y realizar periódicamente análisis o escaneos de vulnerabilidades para proteger a la organización de mejor manera.

Por último, aunque en este ejercicio las actividades de remediación hacen referencia a configuraciones propias de los protocolos de cifrado, cambio de permisos y la recomendación de compra de certificados de seguridad emitidos por empresas certificadoras, no hay que dejar de lado aspectos tan importantes como los controles en los procesos de calidad y aseguramiento de servicios y servidores a producción por medio de Hardering , la continua revisión de procesos de testing interno y externo de las aplicaciones de una forma más general y exhaustiva en comparación del ejercicio realizado y plasmado en este documento, el cual solo evidencia una porción de un gran objetivo que es asegurar la información.

Sin embargo, no se puede dejar a un lado la importancia de las capacitaciones a los funcionarios en ingeniería social, el cual puede ser el eslabón más débil o más fuerte según su conocimiento de los ataques que los delincuentes informáticos pueden realizar para vulnerar tanto su información como las plataformas propias de la compañía.

Como anexo se adjunta todos los resultados técnicos que hacen parte del proceso de escáner y búsqueda de vulnerabilidades.



Mapa de búsqueda de vulnerabilidades

BIBLIOGRAFÍA

BOLÍVAR, Carlos, El Tiempo.com, “Cinco consejos para estar preparado ante amenazas en la red”, [on line]; Disponible en Internet: http://www.eltiempo.com/archivo/documento/CMS-13981015

CISCO, “Informe Anual de Seguridad Cisco 2016”, [on line]; Disponible en Internet: http://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

DICCIONARIO, Real Academia Española, Disponible en Internet: http://www.rae.es/

FIRMA-E, Consultoría y Desarrollo TI: “Tipos de enfoque en los test de intrusión”, 11 marzo 2013, [on line]; Disponible en Internet: https://www.firma-e.com/blog/que-es-un-test-de-intrusion-1a-parte/

GUÍA DE VULNERABILIDADES CVSS, [on line]; Disponible en internet: https://www.first.org/cvss/user-guide

HACKING, Hacking Ético, Hacktivismo y Seguridad Empresarial - Datos de la actividad Hacker por países, [on line]; Disponible en internet: http://www.gitsinformatica.com/hackers.html

HERZOG Pete, - OSSTMM 2.1 "Manual de Metodología Abierta de Testeo de Seguridad". Última Versión Agosto 23 2003. Disponible en internet: https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/OSSTMM.es.2.1.pdf

INSTITUTO, Nacional de Estándares y Tecnología- Departamento de Comercio de EEUU, Centro de recuses de Seguridad informática, Actualizado 23 de enero de 2017, [on line]; Disponible en internet: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

JARA, Héctor y PACHECO, Federico G: “ETHICAL HACKING 2: Implementación de un sistema de gestión de la seguridad”. 2da Edición, octubre 2013.

MERINO, Marcos, El pentesting como estrategia de seguridad. [on line], 12 marzo 2016, [on line]; Disponible en Internet: http://www.ticbeat.com/seguridad/el-pentesting-como-estrategia-de-seguridad/

MEUCCI, Matteo, “Guía de Pruebas OWASP”, noviembre 2008, [on line]; Disponible en Internet: https://www.owasp.org/images/8/80/Gu%c3%ada_de_pruebas_de_OWASP_ver_3.0.pdf

OPEN, Information Security System Group, “Information Systems Security Assessment Framework ISSFAS Draft 0.2.1A", 1 de mayo del 2006, [on line]; Disponible en Internet: https://ht.transparencytoolkit.org/FileServer/FileServer/whitepapers/issaf/issaf0.2.1A.pdf

OWASP Top 10 -2013 y OWASP Top 10 2017 de los 10 riesgos más críticos en Aplicaciones; entre ellos los riesgos del cifrado no seguro. https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001).

SYMANTEC, Corporation, “Internet Security Threar Report ISTR de Symantec”, Abril de 2017, [on line]; Disponible en Internet: https://www.symantec.com/security-center/threat-report